KVM On The Net™

User Manual

CN6000

FCC Information

This is an FCC Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

RoHS

This product is RoHS compliant.

User Notice

All information, documentation, and specifications contained in this manual are subject to change without prior notification by the manufacturer. The manufacturer makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties as to merchantability or fitness for any particular purpose. Any of the manufacturer's software described in this manual is sold or licensed `as is'. Should the programs prove defective following their purchase, the buyer (and not the manufacturer, its distributor, or its dealer), assumes the entire cost of all necessary servicing, repair and any incidental or consequential damages resulting from any defect in the software.

The manufacturer of this system is not responsible for any radio and/or TV interference caused by unauthorized modifications to this device. It is the responsibility of the user to correct such interference.

The manufacturer is not responsible for any damage incurred in the operation of this system if the correct operational voltage setting was not selected prior to operation. PLEASE VERIFY THAT THE VOLTAGE SETTING IS CORRECT BEFORE USE.

Safety Instructions

General

- Read all of these instructions. Save them for future reference.
- Follow all warnings and instructions marked on the device.
- Do not place the device on any unstable surface (cart, stand, table, etc.). If the device falls, serious damage will result.
- Do not use the device near water.
- Do not place the device near, or over, radiators or heat registers.
- The device cabinet is provided with slots and openings to allow for adequate ventilation. To ensure reliable operation, and to protect against overheating, these openings must never be blocked or covered.
- The device should never be placed on a soft surface (bed, sofa, rug, etc.) as this will block its ventilation openings. Likewise, the device should not be placed in a built in enclosure unless adequate ventilation has been provided.
- Never spill liquid of any kind on the device.
- Unplug the device from the wall outlet before cleaning. Do not use liquid or aerosol cleaners. Use a damp cloth for cleaning.
- The device should be operated from the type of power source indicated on the marking label. If you are not sure of the type of power available, consult your dealer or local power company.
- The device is equipped with a 3-wire grounding type plug. This is a safety feature. If you are unable to insert the plug into the outlet, contact your electrician to replace your obsolete outlet. Do not attempt to defeat the purpose of the grounding-type plug. Always follow your local/national wiring codes.
- Do not allow anything to rest on the power cord or cables. Route the power cord and cables so that they cannot be stepped on or tripped over.
- If an extension cord is used with this device make sure that the total of the ampere ratings of all products used on this cord does not exceed the extension cord ampere rating. Make sure that the total of all products plugged into the wall outlet does not exceed 15 amperes.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or un-interruptible power supply (UPS).

- Position system cables and power cables carefully; Be sure that nothing rests on any cables.
- When connecting or disconnecting power to hot-pluggable power supplies, observe the following guidelines:
  - Install the power supply before connecting the power cable to the power supply.
  - Unplug the power cable before removing the power supply.
  - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supplies.
- Never push objects of any kind into or through cabinet slots. They may touch dangerous voltage points or short out parts resulting in a risk of fire or electrical shock.
- Do not attempt to service the device yourself. Refer all servicing to qualified service personnel.
- If the following conditions occur, unplug the device from the wall outlet and bring it to qualified service personnel for repair.
  - The power cord or plug has become damaged or frayed.
  - Liquid has been spilled into the device.
  - The device has been exposed to rain or water.
  - The device has been dropped, or the cabinet has been damaged.
  - The device exhibits a distinct change in performance, indicating a need for service.
  - The device does not operate normally when the operating instructions are followed.
- Only adjust those controls that are covered in the operating instructions. Improper adjustment of other controls may result in damage that will require extensive work by a qualified technician to repair.

Rack Mounting

- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.
- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Make sure that the rack is level and stable before extending a device from the rack.
- Use caution when pressing the device rail release latches and sliding a device into or out of a rack; the slide rails can pinch your fingers.
- After a device is inserted into the rack, carefully extend the rail into a locking position, and then slide the device into the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Ensure that proper airflow is provided to devices in the rack.
- Do not step on or stand on any device when servicing other devices in a rack.

Package Contents

Basic Package

The basic CN6000 package consists of:

- 1 CN6000 KVM on the NET™
- 1 Custom KVM Cable Set
- 1 Rack Mount Kit
- 1 Power Cord
- 1 User Manual*
- 1 Quick Start Guide

Check to make sure that all the components are present and that nothing got damaged in shipping. If you encounter a problem, contact your dealer.

Read this manual thoroughly and follow the installation and operation procedures carefully to prevent any damage to the unit, and/or any of the devices connected to it.

***** Features may have been added to the CN6000 since this manual was printed. Please visit our website to download the most up to date version of the manual.

© Copyright 2006-2007 ATEN® International Co., Ltd.
Manual Part No. PAPE-0227-300G
Printing Date: 02/2007

ATEN and the ATEN logo are registered trademarks of ATEN International Co., Ltd. All rights reserved.
All other brand names and trademarks are the registered property of their respective owners.

Contents

FCC Information ii
User Notice iii
Safety Instructions iv
General iv
Rack Mounting vi
Package Contents vii
Basic Package vii
Optional Equipment vii
About this Manual xi
Conventions xii
ATEN Information xii
Online Registration xii
Online Support xii

1. Introduction

Overview 1
Features 3
System Requirements 4
Components 5
Front View 5
Rear View 6

2. Hardware Setup

Rack Mounting 7
Installation 9

3. Getting Started

Logging In 11
Screen Elements 14

4. Administration

Introduction 15
General 16
Network 17
Access Port 17
IP Address 18
DNS Server 18
Log Server 18
Security 19
Filtering 20
Radius 22
User Manager 24
Customization 26
Firmware 27

5. The Windows Client

Starting Up 29
Operation 31
OSD Control Panel 31
Keystrokes 32
Mouse Synchronization 32
Hotkeys 34
Configuring the Hotkeys 35
Video Adjustment 36
The Message Board 38
The Button Bar 39
Message Display Panel 39
Compose Panel 39
User List Panel 40

6. The Java Client

Introduction 41
Operation 42
The Toolbar 43

7. The Log File

The Log File Screen 49

8. AP Operation

The Administrator Utility 51
Installation 51
Starting Up 52
Logging In 53
The Settings Notebook 55
Uploading Changes 56
General: 57
Network: 58
Security 60
Filtering 61
User Management 63
Customization 65
Upgrading the Firmware 66
The Windows Client 68
Installation 68
Starting Up 69
The Connection Screen 69
The File Menu 71
The Tools Menu 72
Keyboard 72
Config 73

Connecting 74
Operation 75
The Java Client 76
Starting Up 76
Operation 78
The Log Server 79
Installation 79
Starting Up 80
The Menu Bar 81
Configure 81
Events 82
Options 84
The CN6000 List Panel 85
The Event List Window 87

9. Appendix

Specifications 89
IP Address Determination 90
Administrator Login Failure 93
Troubleshooting 94
General Operation 94
The Windows Client 94
Sun Systems 95
The Java Client 96
The Log Server 96
Trusted Certificates 97
Overview 97
Installing the Certificate 98
Certificate Trusted 99

About this Manual

This User Manual is provided to help you get the most from your c/c system. It covers all aspects of installation, configuration and operation. An overview of the information found in the manual is provided below.

Chapter 1, Introduction, introduces you to the CN6000 System. Its purpose, features and benefits are presented, and its front and back panel components are described.

Chapter 2, Hardware Setup, provides step-by-step instructions for setting up your installation, and explains some basic operation procedures.

Chapter 3, Getting Started, describes how to log into the CN6000 with a browser, and explains the functions of the icons and buttons that appear on the opening page.

Chapter 4, Administration, explains the administrative procedures that are employed to configure the CN6000's working environment, as well as how to operate the CN6000 from the local console.

Chapter 5, The Windows Client, explains how to connect to the CN6000 with the Windows Client software, and describes how to use the OSD to access and control the computers connected to the switch.

Chapter 6, The Java Client, describes how to connect to the CN6000 with the Java Client software, and explains how to use the OSD to access and control the computers connected to the switch.

Chapter 7, The Log File, shows how to use the log file utility to view the events that take place on the CN6000.

Chapter 8, AP Operation, describes how to operate the CN6000 using Windows and Java Client application programs, rather than with the browser method.

An Appendix, at the end of the manual provides technical and troubleshooting information.

Conventions

This manual uses the following conventions:

Monospaced	Indicates text that you should key in.
[ ]	Indicates keys you should press. For example, [Enter] means to press the **Enter** key. If keys need to be chorded, they appear together in the same bracket with a plus sign between them: [Ctrl+Alt].
1.	Numbered lists represent procedures with sequential steps.
♦	Bullet lists provide information, but do not involve sequential steps.
→	Indicates selecting the option (on a menu or dialog box, for example), that comes next. For example, Start → Run means to open the *Start* menu, and then select *Run*.
⚠	Indicates critical information.

ATEN Information

Online Registration

You can register your ATEN product at our online e-Support Center: **http://support.aten.com.**

Online Support

- Online technical support is available to ATEN customers through our e-Support center: **http://support.aten.com**.
- Troubleshooting, Documentation (including online manuals), and Software Updates (firmware and drivers) are available at the ATEN website: **http://www.aten.com**.

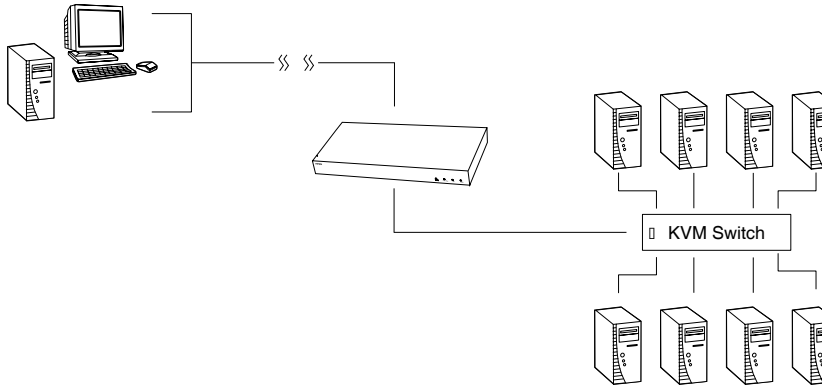
Chapter 1
Introduction

Overview

The CN6000 is a control unit that allows operators to monitor and access their computers from remote locations using a standard Internet browser or Windows-based application programs. The CN6000 connects to the Internet, an Intranet, LAN, or WAN using industry standard Category 5 cable, then uses a KVM cable to connect to a local KVM switch or server.

Because the CN6000 uses TCP/IP for its communications protocol, the server or KVM switch it is connected to can be accessed from any computer on the Net - whether that computer is located down the hall, down the street, or half-way around the world.

Operators at remote locations connect to the CN6000 via its IP address. Once a connection has been established and authorization granted, the remote computer can exchange keyboard, video and mouse signals with the server (or servers on a KVM switch installation), just as if they were physically present and working on the equipment directly.



With its advanced security features, the CN6000 is the fastest, most reliable, most cost effective way to remotely access and manage widely distributed multiple computer installations.

The *Administrator* and *Client* software included with the CN6000 make it easy to install, maintain, and operate. System administrators can handle a multitude of tasks with ease - from installing and running GUI applications, to BIOS level troubleshooting, routine monitoring, concurrent maintenance, system administration, rebooting and even pre-booting functions.

The *Administrator Utility* is available in a both a browser-based version and a Windows-based application version. It is used to configure the system; limit access from remote computers; manage users; and maintain the system with firmware and software module updates.

Both a *Windows GUI Client* and a *Java Client* are also available in browser-based and Windows application versions. They are provided for IP connection and login from anywhere on the net. Inclusion of a Java-based client ensures that the CN6000 is platform independent, and is able to work with all operating systems.

The client software allows access to, and control of, the connected servers. Once an operator successfully connects and logs in, his screen displays what is running on the remote unit attached to the CN6000 (a KVM OSD display, a server's desktop, or a running program, for example) and he can control it from his console just as if he were there.

The *Log Server* records all the events that take place on selected CN6000 units for the administrator to analyze.

Your CN6000 investment is protected by a *Firmware Upgrade Utility*. You can stay current with the latest functionality improvements by downloading firmware update files from our website as they become available, and then using the utility to quickly and conveniently perform the upgrade.

Features

- Remote access of KVM switches or servers via LAN, WAN, or the Internet; control your installation from down the hall, down the street, or half-way around the world
- Supports 10Base-T, 100Base-T, TCP/IP, HTTP
- Advanced security features include password protection and advanced encryption technologies
- High video resolution: up to 1280 x 1024 @ 75Hz; 1600 x 1200 @ 60Hz
- Windows GUI and Java-based client software; Java client works with all operating systems
- Upgradeable firmware via RJ45 Ethernet connection
- Three level password access: Administrator; User; Viewer
- Message board feature allows logged in users to communicate with each other, and allows a user to take exclusive control of the KVM functions
- Supports creation of up to 64 user accounts
- Up to 32 concurrent logins are supported

System Requirements

- For best results we recommend that the computers used to access the CN6000 control unit have at least a P III 1 GHz processor, and that the screen resolution is set to 1024 x 768.
- Browsers must support 128 bit data encryption.
- For best results we recommend that the internet connection speed be at least 128 kbps.
- For the browser-based Windows Client, you must have DirectX 7.0 or higher installed.
- For the browser-based Java Client, you must have Sun's Java 2 (1.4 or higher).
- For the browser-based Log Server, you must have the Microsoft Jet OLEDB 4.0 or higher driver installed.
- Only **non-interlaced** video signals at the following resolutions and refresh rates are supported:

Resolution	Refresh Rates
640 x 480	60, 70, 75, 85, 90, 100, 120
720 x 400	70, 75
800 x 600	56, 60, 70, 75, 85, 90, 100, 120
1024 x 768	60, 70, 75, 85, 90, 100
1152 x 864	60, 70, 75, 85
1280 x 1024	60, 70, 75
1600 x 1200	60

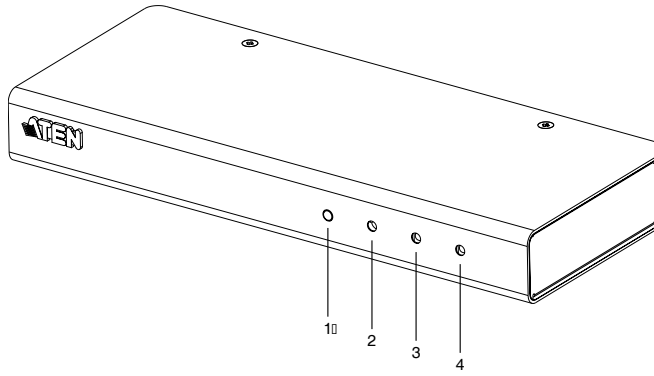
- Only **cable sets** specifically designed to work with the CN6000 may be used. A 1.8 m cable set is provided with this package. Cable sets are also available in other lengths, as shown in the table below.

Length (m)	Part Number
1.2	2L-5201P
1.8	2L-5202P
3.0	2L-5203P
6.0	2L-5206P

If you wish to purchase additional cable sets, contact your dealer.

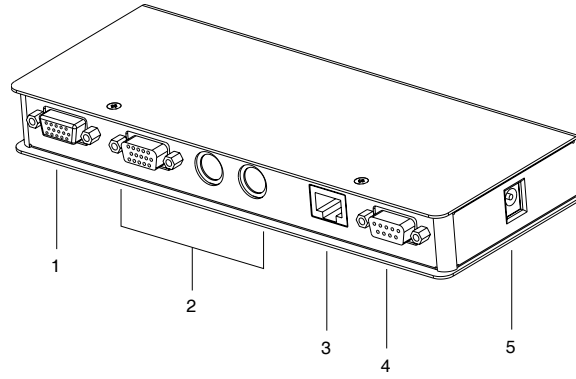
Components

Front View



No.	Component	Description
1.	Reset / Firmware Upgrade Switch	Pressing and holding this switch in while powering ON the CN6000 returns it to the factory default firmware level. After the CN6000 has been powered ON, pressing and holding this switch in for more that two seconds performs a system reset. **Note:** This switch is recessed and must be pushed with a thin object - such as the end of a paper clip, or a ballpoint pen.
2.	Data Speed LED	The LED lights GREEN to indicate 10 Mbps data transmission speed. The LED lights ORANGE to indicate 100 Mbps data transmission speed.
3.	Link LED	Flashes GREEN to indicate that a Client program is accessing the device.
4.	Power LED	Lights ORANGE when the CN6000 is powered up and ready to operate.

Rear View



No.	Component	Description
1.	KVM Port	The KVM cable (supplied with this package) that links the CN6000 to your KVM switch or server plugs in here.
2.	Local Console Section	The CN6000 can be accessed via a local console as well as over the Net. The cables for the local console (keyboard, monitor, and mouse) plug in here. Each port is color coded and marked with an appropriate icon to indicate itself.
3.	RJ-45 Port	The cable that connects the CN6000 to the Internet server plugs in here.
4.	RS-232 Port	The RS-232 port is made available for use with a Power over the NET™ remote power management module. Contact your dealer for details.
5.	Power Jack	The power adapter cable plugs in here.

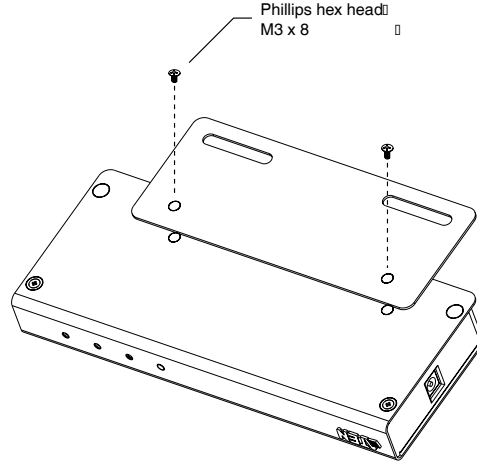
Chapter 2
Hardware Setup

1. Important safety information regarding the placement of this device is provided on page iv. Please review it before proceeding.
2. Make sure that power to all the devices you will be connecting up have been turned off. You must unplug the power cords of any computers that have the Keyboard Power On function.

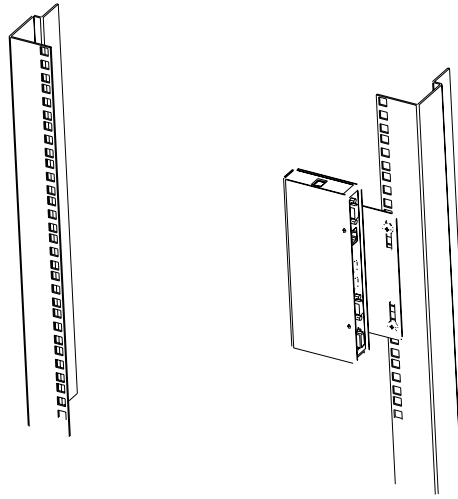
Rack Mounting

For convenience and flexibility, the CN6000 can be mounted on a system rack. To rack mount the unit do the following:

1. Using the screws provided with this package, screw the mounting bracket into the top or bottom of the unit as shown in the diagram below.



2. Screw the bracket into any convenient location on the rack.

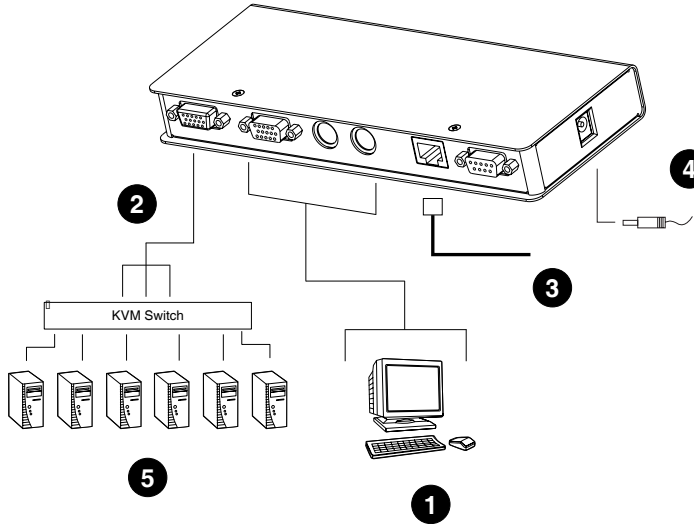


Note: These screws are not provided. We recommend that you use M5 x 12 Phillips Type I cross, recessed type screws.

Installation

To install the CN6000, refer to the diagram below (the diagram numbers correspond to the numbered steps), and do the following:

1. Plug the local administrator's keyboard, mouse, and monitor into the unit's Console Ports.
2. Use the KVM cable provided with this package to connect the CN6000's KVM Port, to the Keyboard, Video and Mouse ports of the server or KVM switch that you are installing.
3. Plug the LAN or WAN cable into the CN6000's RJ-45 socket.
4. Plug the power adapter cable into the CN6000's power jack, then plug the power adapter into an AC power source.
5. Power up your server or KVM installation.



This Page Intentionally Left Blank

Chapter 3
Getting Started

The CN6000 can be accessed either from an internet type browser, or via Windows-based application (AP) programs. The next several chapters describe browser-based operations. AP access is discussed in Chapter 8.

Logging In

To operate the CN6000 from an Internet browser, begin by logging in:

1. Open your browser and specify the IP address of the CN6000 you want to access in the browser's URL location bar.

   Note: 1. Get the IP address from the CN6000 administrator.

   2. If you are the administrator, and are logging in for the first time, the various ways to determine the CN6000's IP address are described in the Appendix on page 90.

2. A *Security Alert* dialog box appears.

Web Site Certified by an Unknown Authority
12:56 06/10
Unable to verify the identity of Aten as a trusted site.
Possible reasons for this error:
- Your browser does not recognize the Certificate Authority that issued the site's certificate.
- The site's certificate is incomplete due to a server misconfiguration.
- You are connected to a site pretending to be Aten, possibly to obtain your confidential information.
Please notify the site's webmaster about this problem.
Before accepting this certificate, you should examine this site's certificate carefully. Are you willing to to accept this certificate for the purpose of identifying the web site Aten?
Examine Certificate...
Accept this certificate permanently
Accept this certificate temporarily for this session
Do not accept this certificate and do not connect to this web site
OK
Cancel
Help

   Accept the certificate – it can be trusted. (See *Trusted Certificates*, page 97, for details.) If a second certificate appears, accept it as well.

The CN6000 login page appears:

3. Provide a valid Username and Password (set by the CN6000 administrator), then Click **Login** to continue.

Note: 1. If you are the administrator, and are logging in for the first time, use the default Username: *administrator*; and the default Password: *password*. For security purposes, we strongly recommend you remove these and give yourself a unique Username and Password (see *User Manager*, page 24).

2. If you supplied an invalid login, the authentication routine will return this message: *Invalid Username or Password. Please try again.* If you see this message, log in again being careful with the Username and Password.

After you have successfully logged in, the CN6000 Main Page appears:

Screen Elements

The icons arranged horizontally across the top of the page are linked to the administration utilities, which are used to configure the CN6000. Your ability to make configuration changes depends on the permissions associated with your login information (see *User Manager*, page 24). Use of the administrative functions is discussed in Chapter 4.

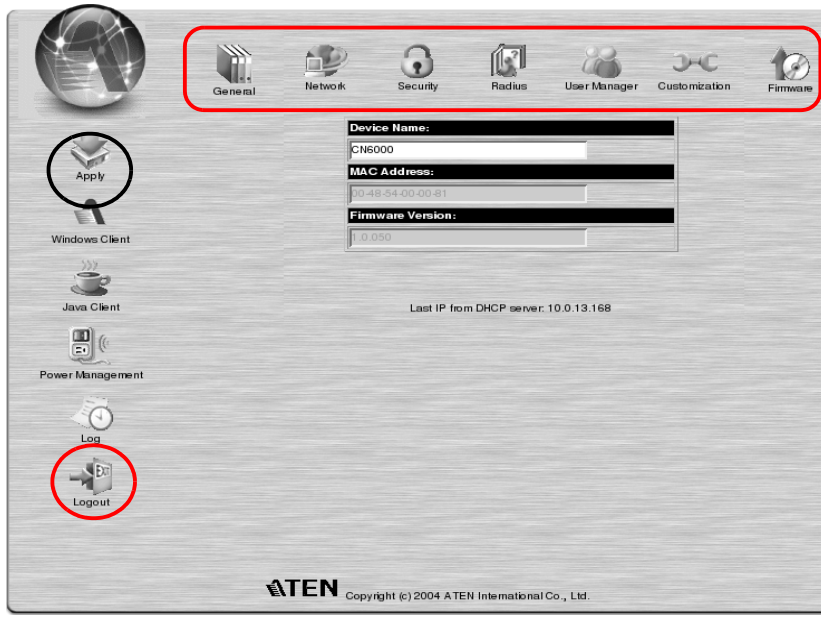
The icons arranged vertically down the left side of the page are used to operate the CN6000. Their purpose is discussed in the table below:

Icon	Purpose
	Saves the changes you make in the administration dialog boxes (see the *Administration* chapter), but does not implement the changes. The changes only go into effect when you enable *Reset on exit* (see *Customization*, page 26) and log out.
	Allows users with the proper permission (see *User Manager*, page 24), to connect to the CN6000 using Windows software, and to remotely control the connected server (or servers via a KVM switch).
	For platform independence, the Java client allows users with the proper permission (see *User Manager*, page 24), that have Java installed to connect to the CN6000 and to remotely control the connected server (or servers via a KVM switch).
	If a Power over the NET™ module is connected to your installation, and if you have the proper permission (see *User Manager*, page 24), clicking this icon will bring up its interface.
	All the events that take place on the CN6000 are recorded in a log file. If you have the proper permission (see *User Manager*, page 24), clicking this icon displays the contents of the log file.
	Click this icon to log out and end your CN6000 session. **Note:** It is important to log out when you end your session. Otherwise, you must wait until the timeout setting has expired before the CN6000 can be accessed again. (See *Time out Control*, page 26.)

Chapter 4
Administration

Introduction

The administration utilities, represented by the icons located across the top of the CN6000 web page, are used to configure the CN6000 for operation.



This chapter discusses each of them in turn. As you make your configuration changes, Click the **Apply** icon at the upper left of the web page to save the changes in the CN6000's configuration file. To have the changes actually take effect, you have to put a check in the *Reset on Exit* box (see *Customization*, page 26), and log out.

Note: If you don't have Configuration privileges (see *User Manager*, page 24), the Administration configuration dialogs are available for viewing, but the input fields are disabled, and cannot be changed.

General

Once you login, the *General* panel displays on the web page:

It is the first of the Administration pages, and provides information about the CN6000's status.

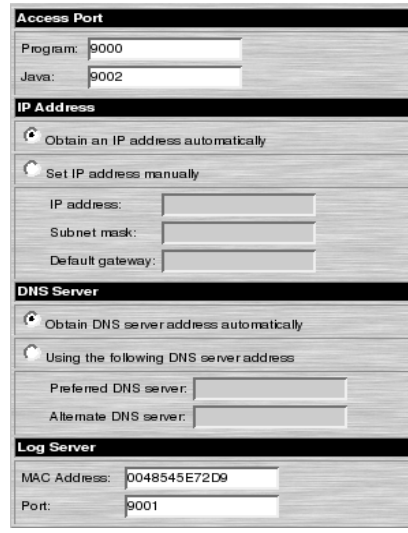
An explanation of each of the fields is given in the table below:

Device Name:	To make it easier to manage installations that have more than one CN6000, each one can be given a name. To assign a name for the CN6000, key in one of your choosing here (15 characters max.).
MAC Address:	The CN6000's MAC Address displays here.
Firmware Version:	Indicates the CN6000's current firmware version level.

Note: New versions of the CN6000's firmware can be downloaded from our website as they become available (see *Firmware*, page 27).

Network

The Network dialog is used to specify the CN6000's network environment.



Access Port

As a security measure, if a firewall is being used, the Administrator can specify the port numbers that the firewall will allow (and set the firewall accordingly). Users must specify the port number as part of the IP address when they log in to the CN6000. If an invalid port number (or no port number) is specified, the CN6000 will not be found.

Note: If there is no firewall (on an Intranet, for example), it doesn't matter what these numbers are set to, since they have no effect.

An explanation of the fields is given in the table below:

Program:	This is the port number that must be specified when connecting from the Administrator and Windows Client software programs. Valid entries are from 1024—60,000.
Java:	This is the port number used for Java Client connections. Valid entries are from 0—65535.

IP Address

The CN6000 can either have its IP address assigned dynamically at bootup (DHCP), or it can be given a fixed IP address.

- For dynamic IP address assignment, select the *Obtain an IP address automatically*, radio button.

> **Note:** If the CN6000 is on a network that uses DHCP to assign network addresses, and you need to ascertain its IP address, see *IP Address Determination*, page 90, for information.

- To specify a fixed IP address, select the *Set IP address manually*, radio button and fill in the IP address.

DNS Server

The CN6000 can either have its DNS server address assigned automatically, or a fixed address can be specified.

- For automatic address assignment, select the *Obtain DNS server address automatically*, radio button.
- To specify a fixed address, select the *Use the following DNS server address*, radio button and fill in the required information.

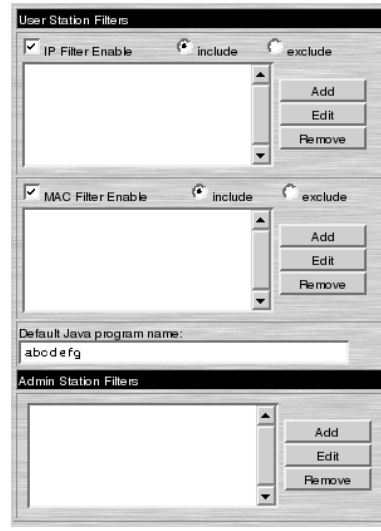
Log Server

Important transactions that occur on the CN6000, such as logins and internal status messages, are kept in an automatically generated log file.

Specify the MAC address and a Port number for the server you want the log server software to reside on.

Security

The Security page is used to control access to the CN6000.



- *IP* and *MAC Filters* permit or deny access to the CN6000 for specific IP and MAC addresses attempting to access the system.
- The *Default Java program name* lets the Administrator specify an addition to the IP address that the user must include when he accesses the CN6000 with the Java Client. For example:

  ```
  192.168.0.126/abcdefg
  ```

  Users must include this name in the IP address, or they will not be granted access.

Note: 1. If nothing is specified here, no one will be able to access the CN6000 with the Java Client.

2. For security purposes, we recommend that you change the name of this page from time to time.

- *Admin station filters* are only supported in the AP version of the Administrator Utility. See *Security*, page 60 for a detailed description.

Filtering

There are a maximum of 100 filters allowed for each category: User IPs; User MACs; and Administrator MACs. User Station filtered items (IPs and MACs) can be specified as included or excluded by highlighting the item and clicking the *include* or *exclude* radio button.

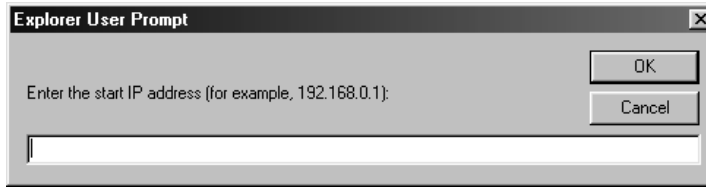
- If the *include* button is checked, all the addresses within the filter range are allowed access to the CN6000; all other addresses are denied access.
- If the *exclude* button is checked, all the addresses within the filter range are denied access to the CN6000; all other addresses are allowed access.

User Station Filtering - IPs:

To enable IP filtering for User Stations, **Click** to put a check mark in the *IP Filter enable* checkbox.

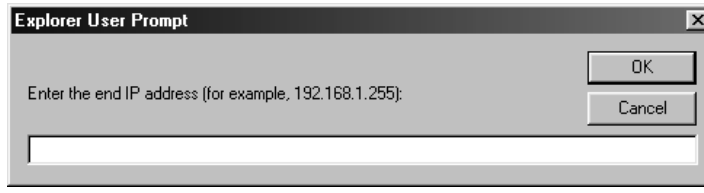
To add a filter:

1. Select whether to include or exclude the filter.
2. Click **Add**. A dialog box similar to the one below appears:



3. Specify the filter address in the dialog box, then Click **OK**.

   Each IP filter can consist of a single address, or a range of addresses. Therefore, a second dialog box similar to the one below appears:



4. To filter a single IP address, key in the same address as the start IP. To filter a continuous range of addresses, key in the end number of the range. After filling in the address, click **OK**.

5. Repeat these steps for any additional IP addresses you want to filter.

To delete a filter, select it and Click **Remove**. To modify a filter, select it and Click **Edit**. The *Edit* dialog box is similar to the *Add* dialog box. When it comes up, simply delete the old address and replace it with the new one.

User Station Filtering - MACs:

To enable MAC filtering for User Stations, **Click** to put a check mark in the *MAC Filter enable* checkbox.

To add a filter:

1. Select whether to include or exclude the filter.

2. Click **Add**. A dialog box similar to the one below appears:

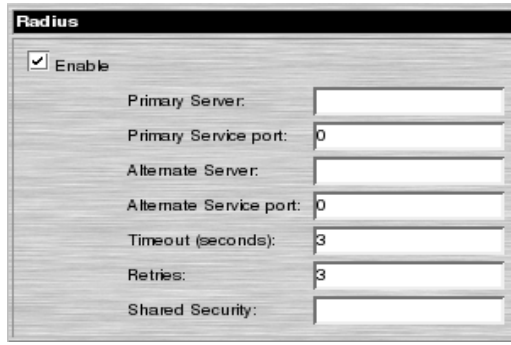
3. Specify the filter address in the dialog box, then Click **OK**.

4. Repeat these steps for any additional MAC addresses you want to filter.

To delete a filter, select it and Click **Remove**. To modify a filter, select it and Click **Edit**. The *Edit* dialog box is similar to the *Add* dialog box. When it comes up, simply delete the old address and replace it with the new one.

Radius

If you are using a RADIUS server, RADIUS Configuration allows you to set up its parameters:



1. Check Enable RADIUS.
2. Fill in the IP addresses and Service Ports for the Primary and Alternate RADIUS servers.
3. Set the time in seconds that the CN6000 waits for a RADIUS server reply before it times out in the Timeout field.
4. Set the number of RADIUS retries allowed in the Retries field.
5. Key the *Shared Security* character string that you want to use for authentication between the CN6000 and the RADIUS Server in this field.

6. On the RADIUS server, set the access rights for each user according to the information in the table, below:

Character	Meaning
C	Grants the user administrator privileges, allowing the user to configure the system.
W	Allows the user to access the system via the Windows Client program.
J	Allows the user to access the system via the Java Client program.
P	Allows the user to access an attached PN0108 device.
L	Allows the user to access log information via the user's browser.
V	Limits the user's access to only viewing the video display.

Note: 1. The characters are not case sensitive. Capitals or lower case work equally well.

2. Characters are comma delimited.

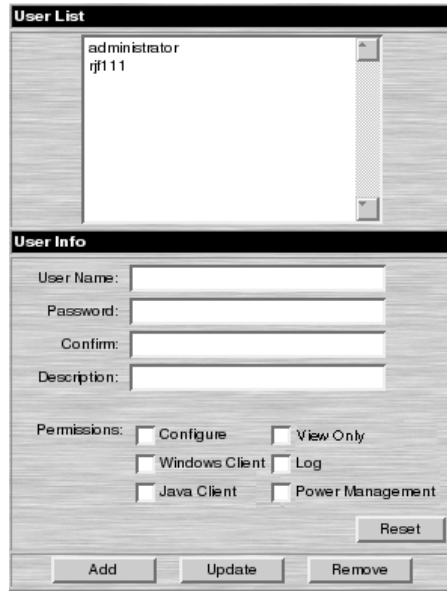
3. An invalid character in the configuration string will prohibit access to the CN6000 for the user.

Examples:

String	Meaning
c,w,p	User has administrator privileges; user can access the system via the Windows Client; user can access the attached PN0108
w,j,l	User can access the system via the Windows Client; user can access the system via the Java Client; user can access log information via the user's browser.

User Manager

This configuration dialog is used to manage user profiles.



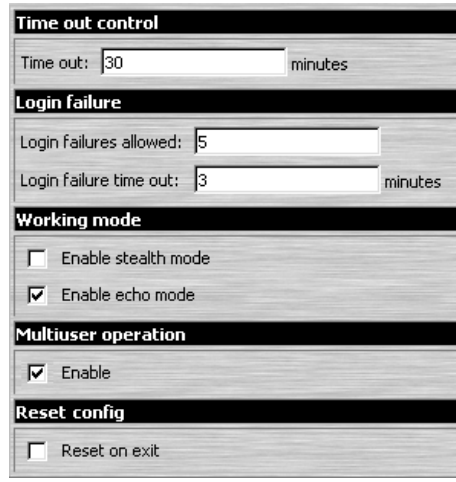
- A maximum of 64 user profiles can be created.
- To add a user, fill in the information asked for in the *User Info* dialog box and Click **Add**.
- To delete a user profile, select it from the list in the upper panel, and Click **Remove**.
- To modify a user profile, select it from the list in the upper panel; change the information shown in the *User Info* dialog box; and Click **Update**.
- The **Reset** button clears all the information shown in the *User Info* dialog box fields.

An explanation of the profile items is given in the table below:

Username	A minimum of 6 and a maximum of 15 characters is allowed.
Password	A minimum of 8 and a maximum of 15 characters is allowed.
Confirm Password	To be sure there is no mistake in the password you are asked to enter it again. The two entries must match.
Description	Additional information about the user that you may wish to include.
Permissions	Click to place/remove a check mark next to an item to grant/withhold access to that aspect of the CN6000's operation. **Configure:** Checking *Configure* gives a User Administrator priveleges, and allows the user to set up and modify the CN6000's operating environment. **Windows Client:** Checking *Windows client* allows a User to access the CN6000 via the Windows Client software. **Java Client:** Checking *Java client* allows a User to access the CN6000 via the Java Client software. **View Only:** Checking *View Only* allows a User to view the video of the display of the computers attached to the ports of the KVM switch connected to the CN6000, but they are not allowed to perform any operations on the computers. **Log:** Checking *Log* allows a User to view the contents of the log file. **Power Management:** Checking *Power Management* allows a User to access and operate an attached Power over the Net™ module.

Customization

This configuration dialog allows the Administrator to set *Timeout*, *Login failure*, and *Working mode* parameters.



An explanation of the Customization parameters is given in the table below:

Time out Control	If the CN6000 doesn't receive any input from a computer that is accessing it with the Windows or Java client for the amount of time specified here, it ends the connection.
Login failure	*Login failures allowed*, sets the number of consecutive failed login attempts that are permitted from a remote computer. *Login failure timeout*, sets the amount of time a remote computer must wait before attempting to login again after it has exceeded the number of allowed failures.
Working Mode	If *Stealth Mode* is **enabled**, the CN6000 cannot be pinged. If *Echo Mode* is **disabled**, the CN6000 will not show up in the list of local CN6000 units. See the CN6000 AP version manual (provided on the CD that came with this package) for details.
Multiuser Operation	Enabling Multiuser operation permits more than one user to log into the CN6000 at the same time.
Reset on exit	Placing a check here causes the CN6000 to reset itself and implement all the new changes when you log out. A wait of approximately 30 to 60 seconds is necessary before logging in following the reset.

Firmware

New versions of the CN6000 firmware can be downloaded from our website:

`www.aten.com.tw`

as they become available. To upgrade the firmware, do the following:

1. After downloading the new firmware file to your computer, click the *Firmware* icon to open the Firmware configuration dialog:

2. Click the Browse button; navigate to the directory that the new firmware file was downloaded to, and select it.
3. Click **Upload**.
4. After the upload completes, click the *Apply* icon at the left of the web page.
5. Enable the *Reset on exit* checkbox (See *Customization*, page 26).
6. Click the *Apply* icon at the left of the web page, again.
7. Click the **Logout** icon at the upper right of the web page (see page 12) to exit and reset the CN6000.

This Page Intentionally Left Blank

Chapter 5
The Windows Client

Starting Up

To access the CN6000 with the Windows Client software:

1. After you log in, Click the *Windows Client* icon at the left of the web page (see page 12).

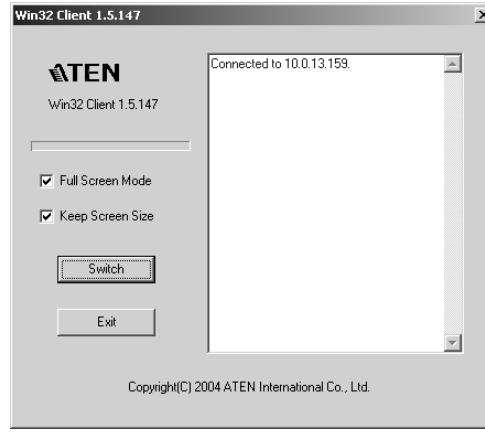
   Note: You must have DirectX 7.0 or higher installed on your computer. If not, the Client program will not load.

2. In the dialog box that comes up, click **Open** to run the program.

   Note:.1. If the browser cannot run the program, save it to disk, instead. Then, with your browser still open to the CN6000 web page, run the file from your disk.

   2. If you use the *save to disk* method, for security purposes, you cannot simply run a previously downloaded version of the program. Each time you want to access the CN6000, you must log in to the web page with a valid username and password to download a fresh copy of the program.

3. When a connection to the CN6000 has been established, a screen similar to the one below appears:



An explanation of the dialog box is given in the table below:

Element		Action
Full Screen Mode	Enabled	If *Full Screen Mode* is enabled (there is a checkmark in the box), the remote display fills the entire screen of your local monitor.
	Disabled	If *Full Screen Mode* is not enabled (there is no checkmark in the box), the remote display appears as a window on your desktop. If the remote screen is larger than what is able to fit in the window, move the mouse pointer to the screen border that is closest to the area you want to view and the screen will scroll. Clicking the push pin icon in the title bar will cause the window to remain on top of all other open windows on your desktop.
Keep Screen Size	Enabled	If *Keep Screen Size* is enabled (there is a checkmark in the box), the remote screen is not resized.
	Disabled	If *Keep Screen Size* is not enabled (there is no checkmark in the box), the remote screen is resized to fit the resolution of your local monitor. ◆ If the remote resolution is smaller, its display appears as a window centered on your screen. ◆ If the remote resolution is larger, its display is centered on your screen. To access the areas that are off screen, move the mouse to the corner of the screen that is closest to the area you want to view and the screen will scroll.
Switch		Click **Switch** to take over console control of the unit that the CN6000 is connected to.
Exit		Click to exit the Windows Client program.

Operation

Once the Switch to the CN6000 has been accomplished, the remote system's video output is captured and displayed on your monitor. At the same time, your local keystroke and mouse input is captured and sent to the remote system.

OSD Control Panel

A small OSD control panel opens at the lower right hand corner of the screen:

The panel consists of an icon bar with two text bars below it. Initially, the text bars display the video resolution and IP address of the remote device. As the mouse moves over the icons, the text bars describe the icon's function. The functions that the icons perform is described in the table below.

Icon	Function
	Click and drag the hand to move the OSD display to another position on the screen.
	Click to bring up the Hotkey Setup dialog box (see page 34 for details).
	Click to bring up the Video Adjustment dialog box. Right click to do a fast Auto Sync (see page 36 for details).
	Click to open the Message Board (see page 38 for details).
	Click to exit the Windows Client control of the remote unit.
(Space)	Hover over the space to see the video resolution and IP address of the device at the remote location.
	These LEDs show the Num Lock, Caps Lock, and Scroll Lock status of the remote computer. Click on the icon to toggle the status. **Note:** When you first connect, the LED display may not be accurate. To be sure, click on the LEDs to set them.

Keystrokes

Except for **[Alt + Tab]** and **[Ctrl + Alt + Del]**, the effect of all keyboard input takes place on the remote computer . The above two combinations are retained on the local system to switch among applications and to recover from disaster. In order to provide the [Alt + Tab] and [Ctrl + Alt + Del] functions on the remote system, a Function key (F1 - F12) can be selected as a substitute for the [Alt] key.

For example, if you choose [F12] as the substitute, then **[F12 + Tab]** would switch among apps on the remote system, and **[Ctrl + F12 + Del]**, would be the disaster recovery combination. See *Configuring the Hotkeys*, page 35, for details on setting up a substitute key.

Note: While any Function Key can be used for the Substitute key, you ***must not*** use one that is being used for another action.

Mouse Synchronization

Until you close the CN6000 connection, mouse movements have no effect on your local system, but are captured and sent to the remote system, instead.

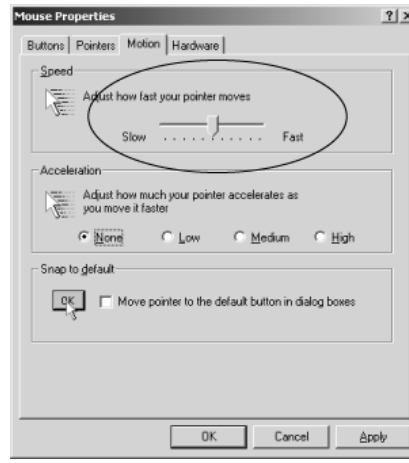
From time to time, especially if you change video resolution, the local mouse movement may no longer be synchronized with the remote system's mouse pointer. There are three quick methods that can be used to bring the two pointers back into sync: 1) Moving the mouse pointer over the Arrow in the OSD panel and right clicking; 2) Moving the mouse pointer into the OSD panel and then moving it back out again; and 3) Performing an *Auto Sync* with the Video Adjustment function (see *Video Adjustment*, page 36). If performing these actions doesn't resolve the problem, do the following:

1. Invoke the *Adjust Mouse* action with the *Adjust Mouse* hotkeys (see page 34 for details).
2. Move the local mouse pointer exactly on top of the remote mouse pointer and **Click**.

If these procedures still do not help, set the mouse speed and acceleration for the computer (or computers via KVM switch) connected to the CN6000 as follows:

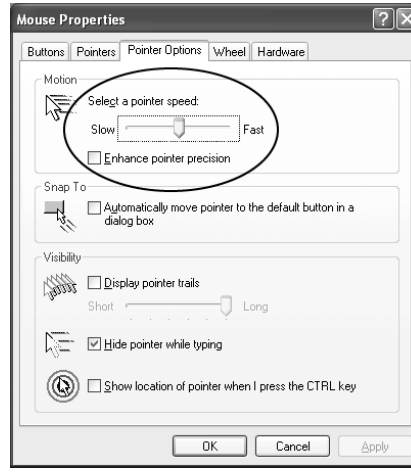
Windows 2000:

Set the mouse speed to the middle position; set the mouse acceleration to *None* (Control Panel → Mouse → Mouse Properties → Motion):



Windows XP/Server 2003:

Set the mouse speed to the middle position; disable *Enhance Pointer Precision* (Control Panel → Printers and Other Hardware → Mouse → Pointer Options):



WinMe:

Set the mouse speed to the 5th position; disable mouse acceleration (click Advanced to get the dialog box for this).

WinNT / Win98 / Win95:

Set the mouse speed to the slowest position.

Sun / Linux:

Open a terminal session and issue the following command:

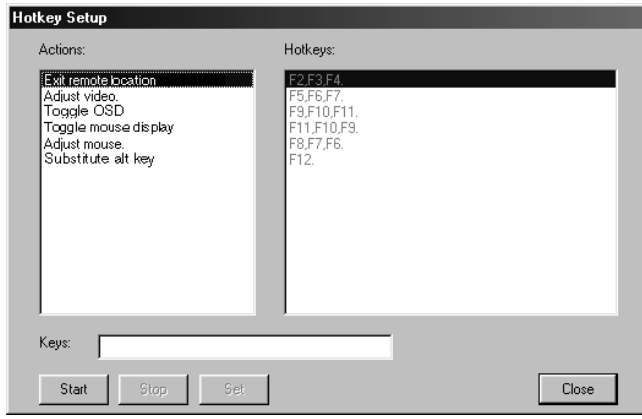
Sun: xset m 1

Linux: xset m 0

Hotkeys

The Hotkey Setup Screen:

Various configuration actions related to the keyboard, video, and mouse can be performed via hotkey combinations. The Hotkey setup utility is accessed by clicking the *Keyboard* icon on the OSD Control Panel. The actions performed by the Hotkeys are listed in the left column; the currently defined keys that invoke the actions are shown in the column to the right.



An explanation of the actions is given in the table, below:

Action	Explanation
Exit remote location	Break the connection to the CN6000 and return to local operation.
Adjust Video	Bring up the video adjustment utility.
Toggle OSD	Toggles the OSD display Off and On.
Toggle mouse display	If you find the display of the two mouse pointers (local and remote) to be confusing or annoying, you can use this function to shrink the non-functioning pointer down to a barely-noticeable tiny circle - which can be ignored. Since this function is a toggle - use the hotkeys again to bring the mouse display back to its original configuration.
Adjust mouse	This utility synchronizes the local and remote mouse movements following a video resolution change. After invoking this utility, simply click the local mouse pointer on top of the remote mouse pointer.
Substitute Alt key	Although all other keyboard input is captured and sent to the CN6000, [Alt + Tab] and [Ctrl + Alt + Del] work on your local computer. In order to implement their effects on the remote system, a function key is be substituted for the Alt key. If you substitute the F12 key, for example, you would use [F12 + Tab] and [Ctrl + F12 + Del].

Note: To invoke an action, you must press and release the keys one key at a time – do not *chord* the keys.

Configuring the Hotkeys

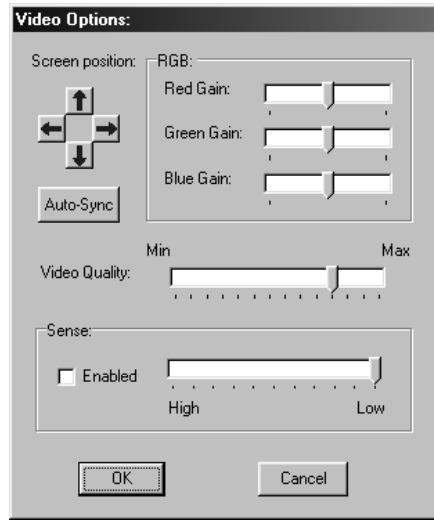
If you find the default Hotkey combinations inconvenient, you can configure them to whatever suits your taste, as follows:

1. Highlight the Action, then Click **Start**
2. Key in the Function keys (one at a time). The key names appear in the *Key* field as you press them.
3. When you have finished keying in your sequence, Click **Stop**
4. Click **Set**
5. Repeat for any other actions you wish to set up

Note: You can use the same function keys for more than one action, ***as long as the first key is not the same***. For example, you can use **F1 F2 F3** for one action; **F2 F1 F3** for another; **F3 F2 F1** for a third, etc.

Video Adjustment

You can adjust the placement and the picture quality of the remote screen (as displayed on your local monitor) with the Video Options function. To do so, either click on the Hammer icon on the OSD Control Panel, or use the *Adjust Video* hotkeys (see page 34 for details). The following screen appears:



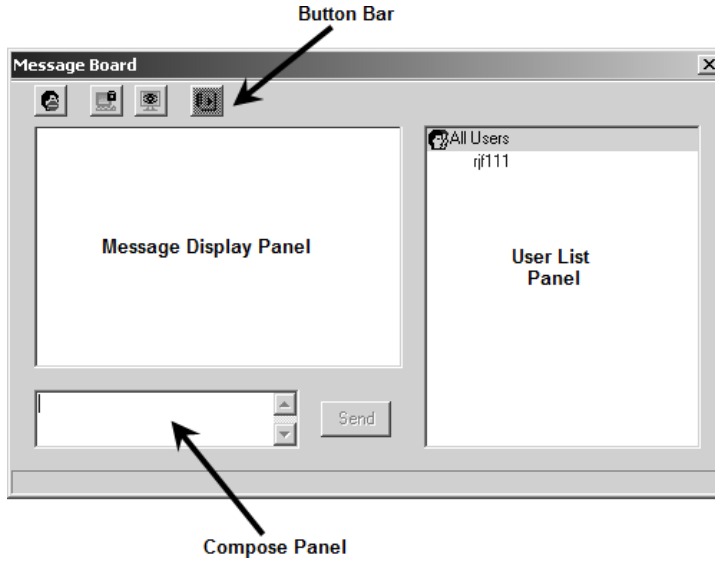
The meanings of the adjustment options are given in the table below:

Option	Usage
Screen Position	Adjust the horizontal and vertical position of the remote computer window by Clicking the Arrow buttons.
Auto-Sync	Click Auto-Sync to have the function detect the vertical and horizontal offset values of the remote screen and automatically synchronize it with the local screen. If the local and remote mouse pointers are out of sync, in most cases, performing this function will bring them back into sync. **Note:** This function works best with a bright screen. If you are not satisfied with the results, use the Screen Position arrows to position the remote display manually.
RGB	Drag the slider bars to adjust the RGB (Red, Green, Blue) values. When an RGB value is increased, the RGB component of the image is correspondingly increased.
Video Quality	Drag the slider bar to adjust the overall Video Quality. Values can be from 20 to 100. The larger the value, the clearer the picture and the more video data goes through the network. Depending on the network bandwidth, a high value may adversely effect response time.
Sense	If you need to adjust the gamma level of the remote video display, put a check mark in the *Enable* box, then drag the slider bar until the desired result is obtained.

The Message Board

The CN6000 supports multiple user logins, which can possibly give rise to access conflicts. To alleviate this problem, a message board feature has been provided, allowing users to communicate with each other.

The message board functions much like an internet chat program does. When you click the Message Board icon on the Windows Client toolbar (see page 31), a screen similar to the one below appears:



The Button Bar

The buttons on the Button Bar are toggles. Their actions are described in the table below:

Button	Action
	Enable/Disable Chat. When disabled, messages posted to the board are not displayed. The button is shadowed when Chat is disabled. The icon displays next to the user's name in the User List panel when he has disabled Chat.
	Occupy/Release Keyboard/Video/Mouse. When you Occupy the KVM, other users cannot see the video, and cannot input keyboard or mouse data. The button is shadowed when the KVM is occupied. The icon displays next to the user's name in the User List panel when he has occupied the KVM.
	Occupy/Release Keyboard/Mouse. When you Occupy the KM, other users can see the video, but cannot input keyboard or mouse data. The button is shadowed when the KM is occupied. The icon displays next to the user's name in the User List panel when he has occupied the KM.
	Show/Hide User List. When you Hide the User List, the User List panel closes. The button is shadowed when the User List is open.

Message Display Panel

Messages that users post to the board - as well as system messages - display in this panel. If you disable Chat, however, messages that get posted to the board won't appear.

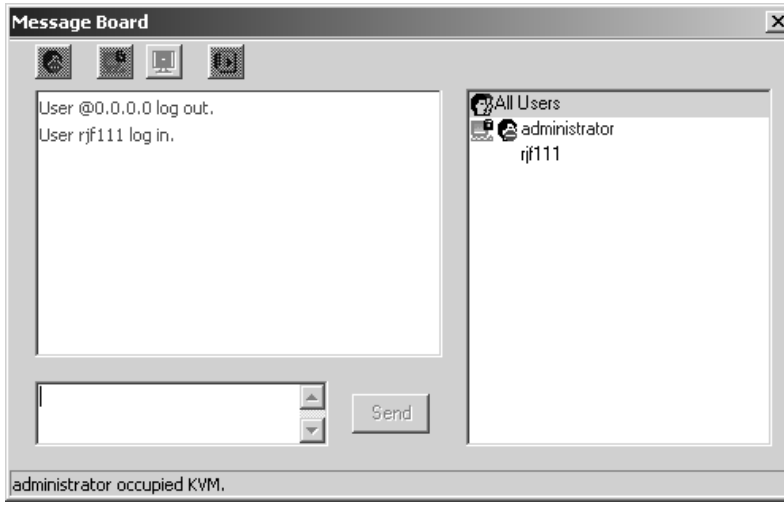
Compose Panel

Key in the messages that you want to post to the board in this panel. Click **Send**, or press **[Enter]** to post the message to the board.

User List Panel

The names of all the logged in users are listed in this panel.

- Your name appears in olive; other users' names appear in green.
- By default, messages are posted to all users. To post a message to one individual user, select the user's name before sending your message.
- If a user's name is selected, and you want to post a message to all users, select *All Users* before sending your message.
- If a user has disabled Chat, its icon displays before the user's name to indicate so.
- If a user has occupied the KVM or the KM, its icon displays before the user's name to indicate so.



Chapter 6
The Java Client

Introduction

The Java Client makes the CN6000 accessible to all platforms that have Java 2 installed. Java 2 is available for free download from Sun's Java web site (http://java.sun.com). To access the CN6000 with the Java Client software:

1. After you log in (see page 11), Click the *Java Client* icon.

   Note: When you log in, be sure to specify the *Java Program Name* when you specify the CN6000's IP address. For example:
   192.168.0.125/abcdefg
   Otherwise you will not be granted access. If you don't know the program name, get it from your Administrator.

2. In the dialog box that appears, select *Open*.

   Note: If the browser won't open the Java Client program, save the program to disk and, with your browser still open, *Launch* it after the save.

   After a second or two, an *Authentication* progress window appears:

Java Client 1.5.147
JAVA CLIENT Version 1.0.060
Welcome to the Java Client
Now you can access your remote KVM or servers from your local console via the internet.
CN-6000
Initializing...
Cancel

Once the authentication procedure completes successfully, the remote system displays on your monitor:

Operation

You can work on the remote system via the screen display on your monitor just as if it were your local system.

Note: 1. You can switch between your local and remote programs with [Alt + Tab].

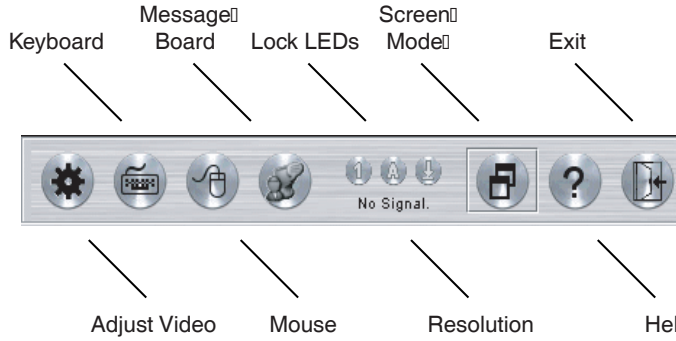
2. Due to *net lag*, there might be a slight delay before your keystrokes show up. You may also have to wait a bit for the remote mouse to catch up to your local mouse before you click.

3. Due to *net lag*, or insufficient computing power on the local machine, some images, especially motion images, may display poorly.

4. If the local and remote mouse pointers get out of sync, you can use the *Mouse Synchronization Button* to bring them back into synch (see page 44 for details).

The Toolbar

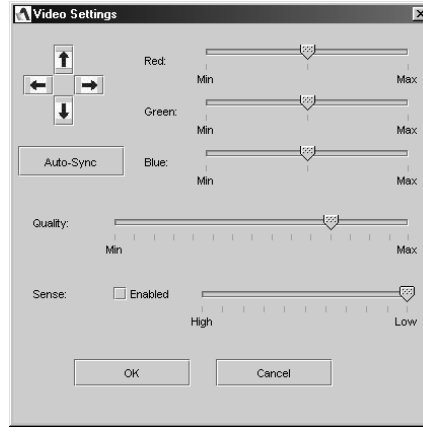
The Java Client's toolbar gives you control over the KVM operations. It is hidden in the blank area at the bottom center of the screen, and appears when you move the mouse pointer over this area.



Going from left to right, the toolbar functions are explained in the sections that follow.

Video:

Clicking the first button brings up the *Video Settings* dialog box:



This is similar to the *Adjust Video* feature of the Windows Client. See p. 36 for details about its use.

Note: We recommend that you perform an Autosync right after you connect for improved mouse synchronization.

Keypad:

Clicking the second button, brings up the Keypad. Since some locally input keyboard combinations can not be captured and sent to the CN6000, the Keypad provides a one-click implementation of their actions on the remote system.

Mouse:

At times the local mouse movement may lose sync with the remote mouse movement. You can try getting them back in sync with a *fast mouse synchronization* by moving the mouse pointer down into the Java Client toolbar. If that doesn't help, do an Autosync (as discussed on the previous page).

If an Autosync doesn't resolve the problem the Mouse Synchronization function can get them back into sync. This is similar to the Mouse Synchronization feature of the Windows Client (see page 32 for details).

1. Click the Mouse Synchronization button.

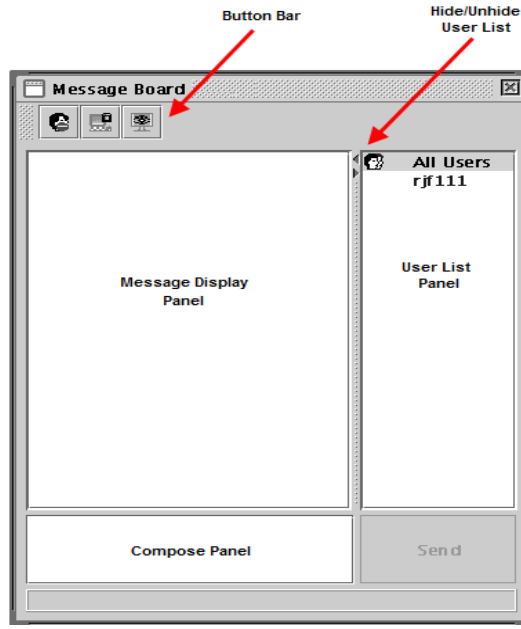
   The remote mouse pointer moves to the upper left area of the screen.

2. Move your local mouse pointer directly over the remote mouse pointer and Click.

Message Board:

The CN6000 supports multiple user logins, which can possibly give rise to access conflicts. To alleviate this problem, a message board feature, similar to an internet chat program allows users to communicate with each other.

When you click the Message Board icon on the Java Client toolbar (see page 43), a screen similar to the one below appears:

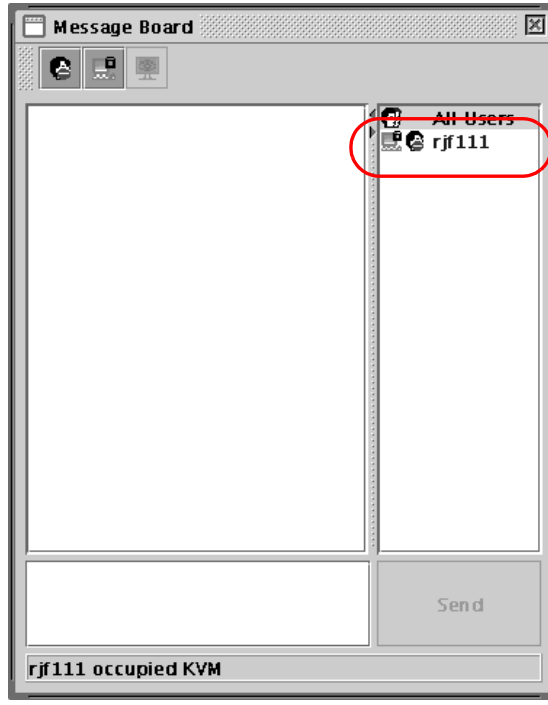


- Messages that users post to the board - as well as system messages - display in the *Message Display* panel. If you disable Chat, however, messages that get posted to the board won't appear.
- Key in the messages that you want to post to the board in the *Compose* panel. Click **Send**, to post the message to the board.
- The names of all the logged in users appear in the *User List* panel.
  - By default, messages are posted to all users. To post a message to one individual user, select the user's name before sending your message.
  - If a user's name is selected, and you want to post a message to all users, select *All Users* before sending your message.
  - To Hide/Unhide the User List panel, click on the arrows in the panel separator.

The buttons on the Button Bar are toggles. Their actions are described in the table below:

	Enable/Disable Chat. When disabled, messages posted to the board are not displayed. The button is shadowed when Chat is disabled. The icon displays next to the user's name in the User List panel when he has disabled Chat.
	Occupy/Release Keyboard/Video/Mouse. When you Occupy the KVM, other users cannot see the video, and cannot input keyboard or mouse data. The button is shadowed when the KVM is occupied. The icon displays next to the user's name in the User List panel when he has occupied the KVM.
	Occupy/Release Keyboard/Mouse. When you Occupy the KM, other users can see the video, but cannot input keyboard or mouse data. The button is shadowed when the KM is occupied. The icon displays next to the user's name in the User List panel when he has occupied the KM.

- If a user has disabled Chat, its icon displays before the user's name to indicate so.
- If a user has occupied the KVM or the KM, its icon displays before the user's name to indicate so.



Lock LEDs:

These LEDs show the Num Lock, Caps Lock, and Scroll Lock status of the remote computer. Click on the icon to toggle the status.

Note: When you first connect, the LED display may not be accurate. To be sure, click on the LEDs to set them.

Screen Mode:

Clicking this button toggles the display between full screen and windowed modes.

The ? Button:

Clicking this button brings up the Java Client Help pages.

Exit:

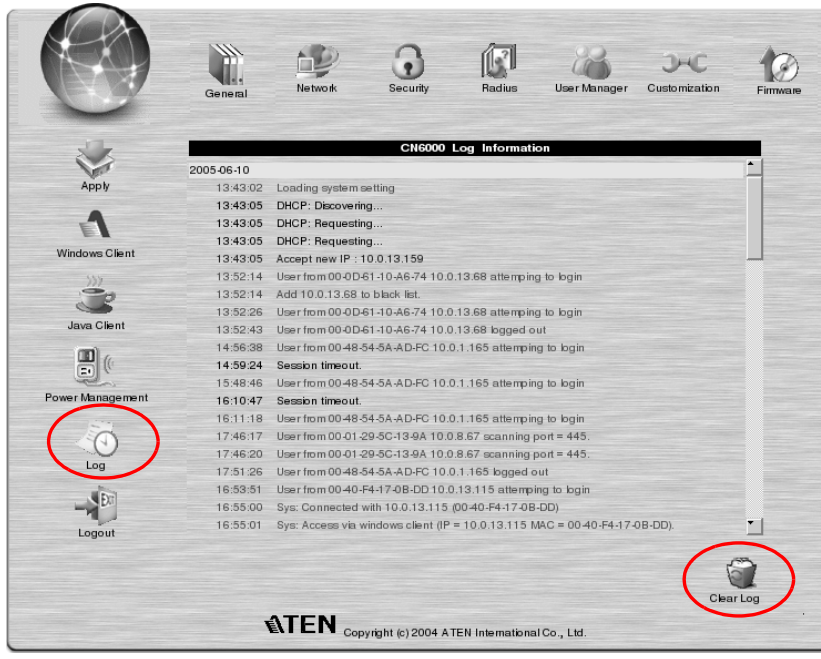
Click this button to exit the Java Client program and return to local operation.

This Page Intentionally Left Blank

Chapter 7
The Log File

The Log File Screen

The CN6000 logs all the events that take place on it. Following a reset, it writes them to a log file, which is a searchable database. To view the contents of the log file, click the *Log* icon at the lower left of the page. A screen similar to the one below appears:


General
Network
Security
Radius
User Manager
Customization
Firmware
Apply
Windows Client
Java Client
Power Management
Log
Logout
CN6000 Log Information
2005-06-10
13:43:02 Loading system setting
13:43:05 DHCP: Discovering...
13:43:05 DHCP: Requesting...
13:43:05 DHCP: Requesting...
13:43:05 Accept new IP : 10.0.13.159
13:52:14 User from 00-0D-61-10-A6-74 10.0.13.68 attemping to login
13:52:14 Add 10.0.13.68 to black list.
13:52:26 User from 00-0D-61-10-A6-74 10.0.13.68 attemping to login
13:52:43 User from 00-0D-61-10-A6-74 10.0.13.68 logged out
14:56:38 User from 00-48-54-5A-AD-FC 10.0.1.165 attemping to login
14:59:24 Session timeout.
15:48:46 User from 00-48-54-5A-AD-FC 10.0.1.165 attemping to login
16:10:47 Session timeout.
16:11:18 User from 00-48-54-5A-AD-FC 10.0.1.165 attemping to login
17:46:17 User from 00-01-29-5C-13-9A 10.0.8.67 scanning port = 445.
17:46:20 User from 00-01-29-5C-13-9A 10.0.8.67 scanning port = 445.
17:51:26 User from 00-48-54-5A-AD-FC 10.0.1.165 logged out
16:53:51 User from 00-40-F4-17-0B-DD 10.0.13.115 attemping to login
16:55:00 Sys: Connected with 10.0.13.115 (00-40-F4-17-0B-DD)
16:55:01 Sys: Access via windows client (IP = 10.0.13.115 MAC = 00-40-F4-17-0B-DD).
Clear Log
ATEN
Copyright (c) 2004 ATEN International Co., Ltd.

A maximum of 512 events are kept in the log file. As new events are recorded, they are placed at the bottom of the list. When a new event is recorded after there are 512 events in the log file, the earliest event in the list is discarded.

Note: To maintain and view a record of all the events that take place (not just the most recent 512), set up the Log Server AP program. See p. 79 for details.

To clear the log file, click on the *Clear Log* icon at the lower right of the page.

Chapter 8
AP Operation

In addition to the browser based operation utilities, the CN6000 also provides Windows-based programs that can be used in their stead. These include an administration utility, a Windows client, a Java client, and a Log Server. This chapter explains how to install and operate each of them.

The Administrator Utility

Installation

The Windows-based Administrator Utility is provided on the distribution CD included with this package. To install the Administrator Utility:

1. Open the drive and folder where the Administrator Setup icon (**CN6KAdminTool.exe**) is located and double click the icon.

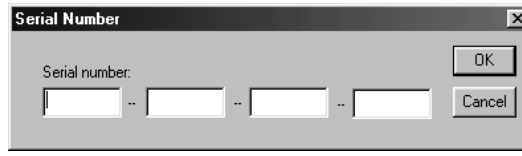
   The Administration Utility installation screen appears:

2. Click **Next** and follow the on-screen instructions. When the installation completes, a *CN6000AdminTool* icon appears on your desktop.

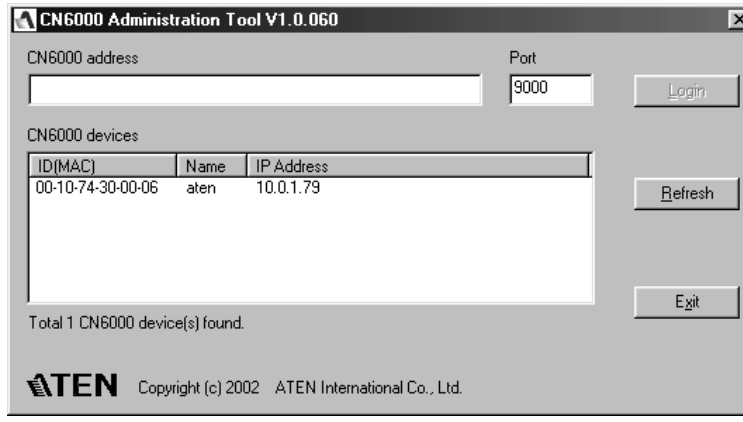
Starting Up

To bring up the Administrator Utility Main Screen, double click the *CN6KAdminTool* icon, or key in the full path to the program on the command line.

If this is the first time that you are running the utility a dialog box appears requesting you to input your serial number. The serial number can be found on the CN6000's CD case. Key in the serial number - 5 characters per box - then Click **OK**



The Administrator Utility searches for CN6000 devices installed on the local LAN segment. When it has finished, it displays the CN6000 devices it found in a window similar to the one below:



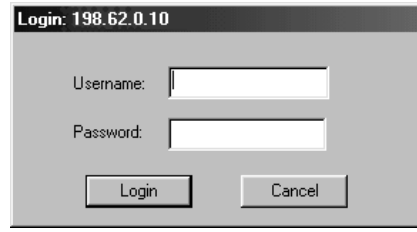
- If the unit you wish to configure appears in the CN6000 *devices* listbox, **Double Click** it.
- If the unit you want doesn't appear in the listbox, key in its IP address in the CN6000 *address* field, and its Port number in the *Port* box, then Click **Login**.

Note: 1. 1.The Port number that corresponds to a unit's IP address is set by the Administrator on the Network configuration page (see page 58 for details).

2. Clicking the **Refresh** button causes the utility to rescan the local LAN segment for CN6000 devices.
3. If the utility fails to connect to a unit that you specified, it assigns another free IP address (if one exists), to that device and attempts to connect again.
4. When the Administrator Utility searches for CN6000 devices, if it finds a unit that was originally on a different network segment that still has a fixed IP address from its previous location, it will list the unit (showing the IP address), but you cannot connect to it. You should change the unit's IP address to match its current network segment (see *IP Address Determination*, page 90, for details).

Logging In

Once the Administrator Utility connects to the unit you specified, a login window appears:

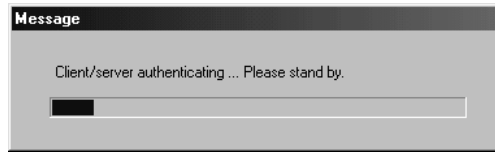


Only those who have Configuration privileges (see *User Management*, page 63) are allowed to log in.

Provide a valid Username and Password, then Click **Login** to continue.

Note: The default Username is *administrator*; the default Password is *password*. You can change these to whatever you prefer (see *User Management*, page 63) after you have logged in.

While the Utility processes the login request, the following message appears:



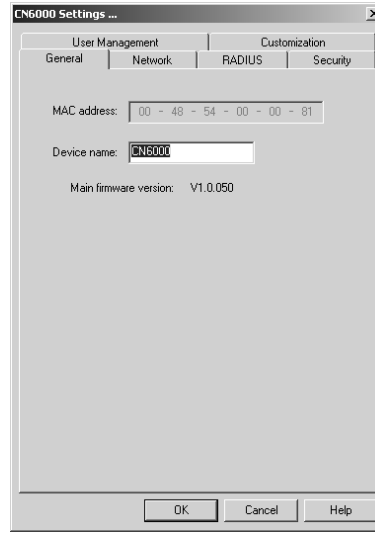
Note: If you supplied an invalid login, the authentication routine will return a message informing you that the "server is busy." This is done as a security measure to confuse and discourage hackers from trying to discover a valid Username and Password. If you see this message, try logging in again being careful with the Username and Password

If you successfully log in to the CN6000 with the default username and password, the following message appears:

For security purposes, be sure to change the default Username and Password to something unique (see *User Management*, page 63).

The Settings Notebook

After successfully logging in, the Settings notebook appears.

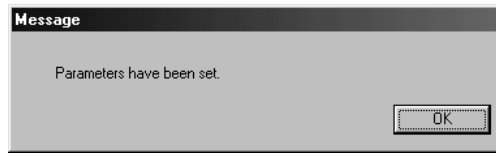


There are five tabs, each representing a different administrative function. A description of the functions and how to configure their settings is provided in the sections that follow.

■ Uploading Changes

When the Settings have been configured to your satisfaction and you are ready to upload the changes to the CN6000:

1. If you made changes on the *Network* page, or if you upgraded the firmware on the *Customization* page, you must enable *Reset on Exit* (see *Customization*, page 65) before going to step 2.
2. Click **OK** (at the bottom of the Settings notebook), to start the updating procedure.When updating has finished, the following message displays:

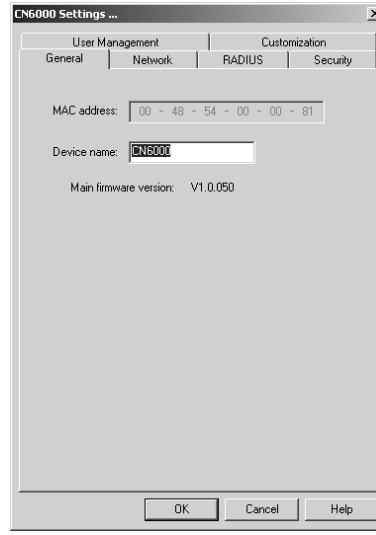


3. Click **OK** and you return to the Administration Utility device selection screen (see page 52).

Note: To abandon the changes you made and return the settings to the values they had before you ran the Utility, Click **Cancel**.(at the bottom of the Settings notebook) instead of OK in step 1.

■ General:

The General page provides information about the CN6000's status.



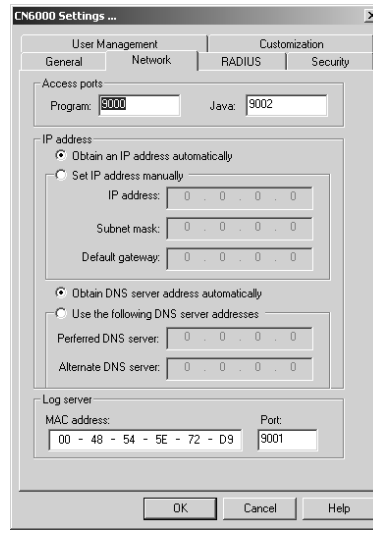
An explanation of each of the items is given in the table below:

MAC Address	The CN6000's MAC Address displays here.
Device Name:	To make it easier to manage installations that have more than one CN6000, each one can be given a name. To assign a name for the CN6000, erase the current name and key in one of your choosing (15 characters max.).
Main Firmware Version:	Indicates the mainboard's current firmware version level.

New versions of the CN6000's firmware can be downloaded from our web site as they become available (see *Upgrading the Firmware*, page 66, for details).

■ Network:

This page is used to specify the CN6000's network environment.



The Network page is divided into three main sections: Access Ports, IP Address, and Log Server. Each section is discussed below.

Access Ports:

As a security measure, the Administrator can set the Port numbers that the User must specify when he attempts to connect to a CN6000's IP address. Unless the correct Port number is given, the CN6000 device will not be found. An explanation of the fields is given in the table below:

Program:	This is the port number that must be specified when connecting from the Administrator and Windows Client software programs. Valid entries are from 1024—60000.
Java:	This is the port number used for Java Client connections. Valid entries are from 0—65535.

IP Address:

- The CN6000 can either have its IP address assigned dynamically at bootup (DHCP), or it can be given a fixed IP address.
  - For dynamic IP address assignment, select the *Obtain an IP address automatically*, radio button.
  - To specify a fixed IP address, select the *Set IP address manually*, radio button and fill in the required information. See *IP Address Determination*, page 90, for detailed information on assigning a fixed IP address
- The CN6000 can either have its DNS address assigned automatically, or a fixed address can be specified.
  - For automatic address assignment, select the *Obtain DNS server address automatically*, radio button.
  - To specify a fixed address, select the *Use the following DNS server address*, radio button and fill in the required information.

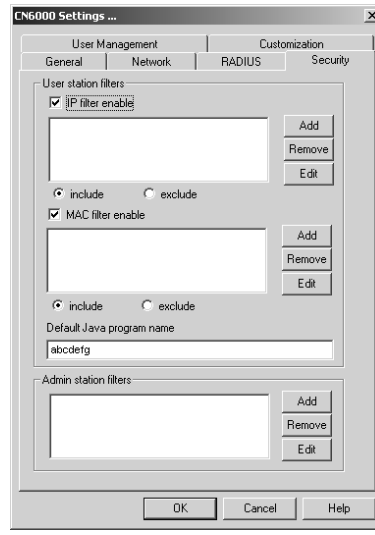
Log Server:

Important transactions that occur on the CN6000, such as logins and internal status messages, are kept in an automatically generated log file. Specify the MAC address and a Port number for the server you want the log file to reside on in the *Log Server* section. The Log Server is discussed in detail on page 79.

Note: The Log Server port number must be different from the port numbers that were specified for Program and Java in the Access Ports section.

■ Security

The Security page is used to control access to the CN6000.



- *User station filters* permit or deny access to the CN6000 for specific IP and MAC addresses attempting to access the system.
- The *Default Java program name* lets the Administrator specify an addition to the IP address that the user must include when he accesses the CN6000 with the Java Client. For example:

  ```
  192.168.0.126/abcdefg
  ```

  Users must include this name in the IP address, or they will not be granted access.

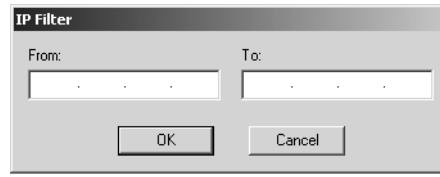
Note: 1. If no page is specified here, no one will be able to access the CN6000 with the Java Client.

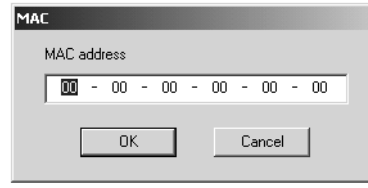
2. For security purposes, we recommend that you change the name of this page from time to time.

- *Admin station filters* specify which MAC addresses are allowed to access the system with the CN6000 Administrator program. If nothing is specified here, there are no restrictions.

Filtering

- There are a maximum of 100 filters allowed for each category (User IPs, User MACs, and Administrator MACs).
- To enable filtering for User Stations, **Click** to put a check mark in the IP and/or MAC *Filter enable* checkbox.
- To add a filter, Click **Add**. A dialog box similar to the ones below appears (the top example is for IP address filters; the bottom is for MAC address filters):

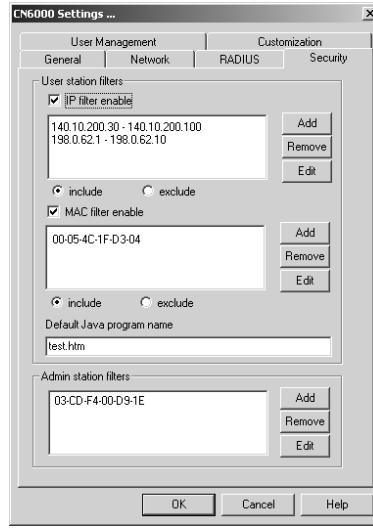




  - Specify the filter address in the dialog box, then Click **OK**.
  - Each filter can consist of a single IP or MAC address, or a range of IP addresses. For a single IP address filter, the address is the same for both the *From* and *To* fields.
- To delete a filter, select it and Click **Remove**; To modify a filter, select it and Click **Edit**. The *Edit* dialog box is similar to the *Add* dialog box. When it comes up, simply delete the old address and replace it with the new one.

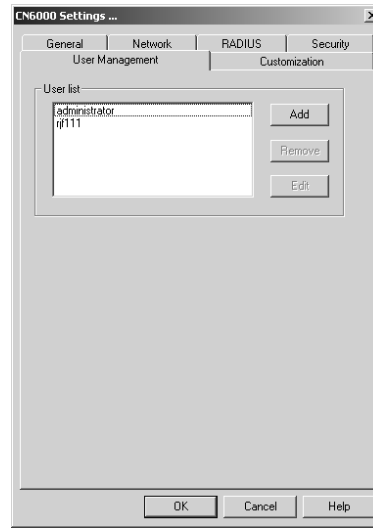
- User Station filtered items can be specified as included or excluded by highlighting the item and clicking the *include* or *exclude* radio button.
  - If the include button is checked, all the addresses within the filter range are allowed access to the CN6000; all other addresses are denied access.
  - If the exclude button is checked, all the addresses within the filter range are denied access to the CN6000; all other addresses are allowed access.
- The Administrator station filter dialog boxes are similar to the MAC filter dialog boxes for user stations.

An example of the Security page with filters configured is shown below:



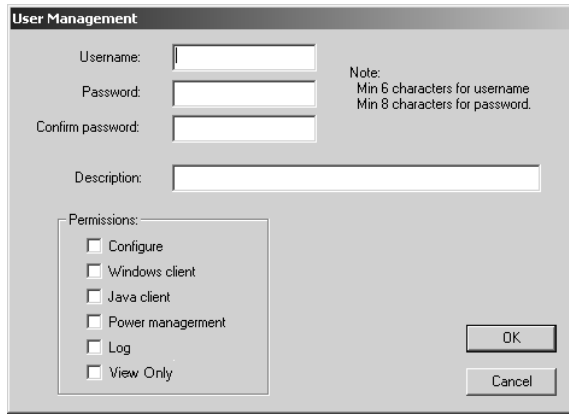
■ User Management

This page is used to set up and manage user profiles. It defines the access rights of each user. Up to 64 user profiles can be established



- A maximum of 64 users can have access to a CN6000.
- To add a user, Click **Add** and fill in the information asked for in the *User Management* dialog box that appears. (See p. 64.)
- To delete a user profile, select it and Click **Remove**.
- To modify a user profile, select it; Click **Edit**; and change the information shown in the *User Management* dialog box that appears.

When you click **Add** or **Edit**, a dialog box with fields to configure the user profile appears:

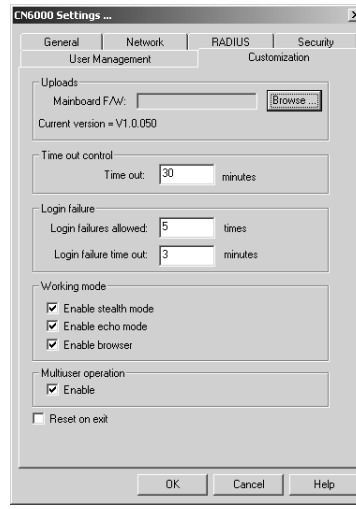


An explanation of the profile items is given in the table below:

Username	A minimum of 6 and a maximum of 15 characters is allowed.
Password	A minimum of 8 and a maximum of 15 characters is allowed.
Confirm Password	To be sure there is no mistake in the password you are asked to enter it again. The two entries must match.
Description	Additional information about the user that you may wish to include.
Permissions	Click to place/remove a check mark next to an item in order to grant/deny access to an aspect of the CN6000's operation as follows: **Configure:** Checking *Configure*gives a User Administrator privileges, and allows the user to set up and modify the CN6000's operating environment. **Windows Client** Checking *Windows client* allows a User to access the CN6000 via the Windows Client software. **Java Client:**Checking *Java client* allows a User to access the CN6000 via the Java Client software. **Power Management:**Checking *Power Management* allows a User to access and operate an attached Power over the Net™ module. **Log:**Checking *Log*allows a User to view the contents of the log file. **View Only:**Checking *View Only* allows the User to view the video display of the computers attached to the ports of the KVM switch connected to the CN6000, but they are not allowed to perform any operations on the computers.

■ Customization

This page allows the Administrator to upgrade the firmware and to set Timeout and Login failure parameters.



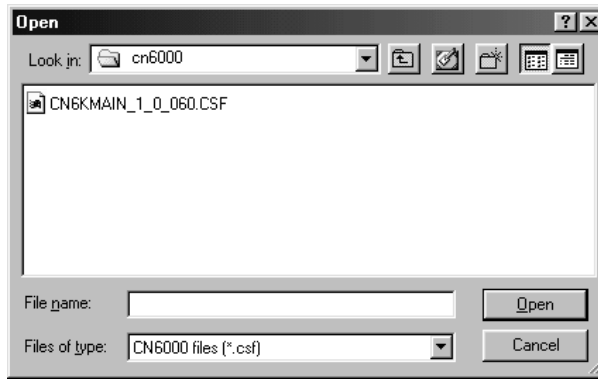
An explanation of the Customization items is given in the table below:

Uploads	After obtaining a new version of the firmware, click **Browse** to navigate to the directory that you have put it in.
Time out control	If the CN6000 doesn't receive any input from a logged in user for the amount of time specified here, it ends the connection.
Login Failure	◆ *Login failures allowed*, sets the number of consecutive failed login attempts that are permitted from a remote computer. ◆ *Login failure timeout*, sets the amount of time a remote computer must wait before attempting to login again after it has exceeded the number of allowed failures.
Working Mode	◆ If *Stealth Mode*is **enabled**, the CN6000 cannot be pinged. ◆ If *Echo Mode*is **disabled**, the CN6000 will not show up in the list of local CN6000 units (see page 52, and page 69). ◆ If *Enable Browser*isn't enabled, the CN6000 cannot be accessed via a browser.
Multiuser operation	Placing a check here allows multiple users to access the CN6000 at the same time. Up to 32 users can log in at the same time this way. **Note:**If you need exclusive access to the CN6000 installation while multiuser sessions are taking place, you can get it from the *Message Board* (see page 38, and page 46).
Reset on exit	Placing a check here causes the CN6000 to reset itself and implement all the new changes when you Click **OK**.

Upgrading the Firmware

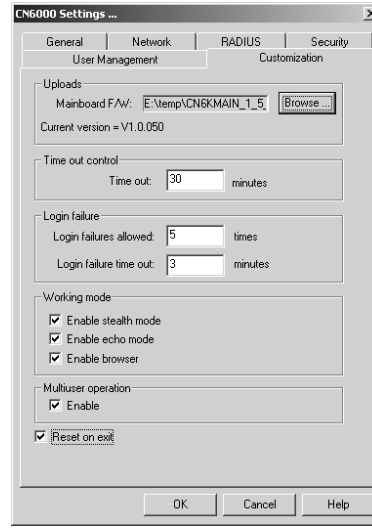
New versions of the Mainboard firmware files can be downloaded from our website as they become available. After downloading the new firmware file, to upgrade the firmware, do the following:

1. Go to the *Customization* page of the Administration configuration notebook (see page 65) and Click the Browse button for the component you want to upgrade.
2. In the *File Open* dialog box that appears, navigate to the directory that the downloaded firmware upgrade file is in, and select the upgrade file.



3. Click **Open**.

   You return to the Customization page with the path to the file, and the Upload version number displayed.



Note: If you select the wrong file type for the component you are upgrading an *Invalid file type* message appears when you click **Open**. Go back and select the correct file type.

4. Enable the *Reset on exit* checkbox.

5. Click **OK** to save your settings and reset the CN6000. Following the reset, wait approximately 30 to 60 seconds before logging back in to the Administrator Utility.

The Windows Client

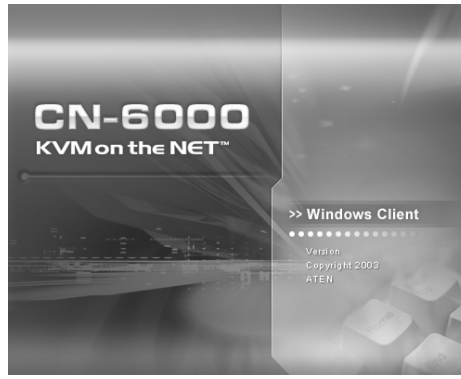
The Windows-based Client software is provided on the distribution CD included with this package.

Installation

To install the Windows Client:

1. Open the drive and folder where the Windows Client Setup icon (**CN6KClient.exe**) is located and double click the icon.

   The Windows Client installation screen appears:

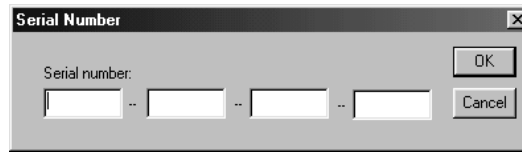


2. Click **Next** and follow the on-screen instructions. When the installation completes, a *CN6000 Client* icon appears on your desktop.

Starting Up

To bring up the Windows Client Main Screen, **Double Click** the *CN6K Client* icon, or key in the full path to the program on the command line.

If this is the first time that you are running the program, a dialog box appears requesting you to input your serial number:

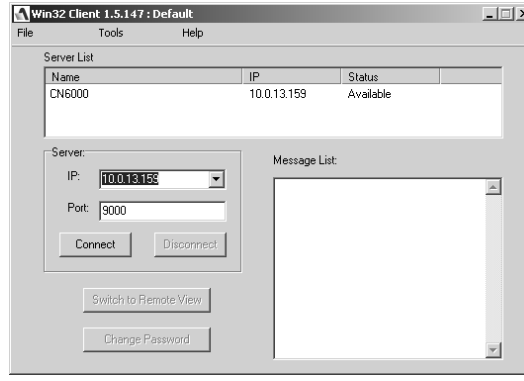


If you don't know what it is, contact the CN6000 administrator. Key in the serial number - 5 characters per box - then Click OK.

Note: You must have DirectX 7.0 or higher installed on your computer. If not, the Client program will not load.

The Connection Screen

When the Windows Client starts, a Connection Screen, similar to the one below, appears:



A description of the Connection Screen is given in the following table:

Menu Bar	The Menu Bar contains three items: File, Tools, and Help. 1. The *File Menu* allows the operator to Create, Save, and Open user created Work files (see page 71 for details). 2. The *Tools Menu* contains two entries:*Keyboard*and *Config*, (see *The Tools Menu*, page 72).
CN6000 List:	Each time CN6KClient.exe is run, it searches the User's local LAN segment for CN6000 units, and lists whichever ones it finds in this box. If you want to connect to one of these units, **Double Click**it.
CN6000 IP:	This area is used when you want to connect to a CN6000 at a remote location. You can drop down the list box and select an IP address or key in an IP address if the one you want isn't listed, then key in the Port number in the *Port* field. If you don't know the Port number contact the Administrator. When the IP address and Port number for the CN6000 unit you wish to connect to has been specified, Click **Connect** to start the connection. When you have finished with your session, Click **Disconnect** to break the connection.
Message List:	Lists status messages regarding the connection to the CN6000.
Switch to Remote View	Once contact with a CN6000 has been established, this button becomes active. Click it to switch and take over console control of the unit that is attached to the CN6000. The screen output of the unit appears on your monitor. Your keystrokes and mouse movements are captured and sent to the CN6000 to be executed on the attached unit. If the CN6000 is connected to a KVM switch, you can control the switch and the computers connected to it just as if you were connected locally.
Change Password	This button becomes active after a connection to a CN6000 unit has been established. It allows the User to change the password he logs onto the CN6000 with.

The File Menu

The *File Menu* allows the operator to Create, Save, and Open user created Work files. A Work File consists of all the information specified in a Client session. This includes the CN6000 and CN6000 IP list items, as well as the Hotkey settings.

Whenever a user runs the Client program, it opens with the values contained in the *current work file*. The current work file consists of the values that were in effect the last time the program was closed.

Users can use the Client program's *File* menu to Create, Save, and Open Work files:

New	Allows the user to create a named work file so its values will not be lost, and it will be available for future recall.
Open	Allows the user to open a previously saved work file and use the values contained in it.
Save	Allows the user to save the values presently in effect as the current work file.

The Tools Menu

Tools menu operations are performed after you connect, but before you switch to remote view. There are two entries on the Tools Menu: Keyboard and Config. They are explained in the sections that follow.

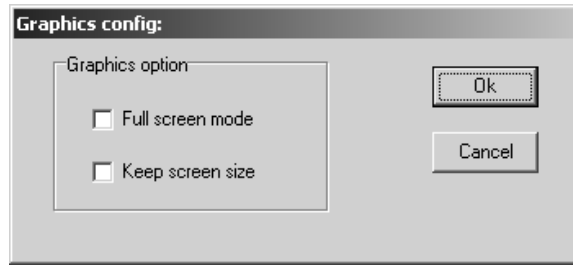
■ Keyboard

Various configuration actions related to the keyboard, video, and mouse can be performed via hotkey combinations. The Hotkey Setup utility is accessed by opening the *Tools* menu and selecting *Keyboard*. The Hotkey Setup Screen appears.

This is essentially the same dialog box discussed in the browser-based *Windows Client* chapter. See *The Hotkey Setup Screen:*, page 34, for details.

■ Config

When you select *Config*, a screen similar to the one below appears:

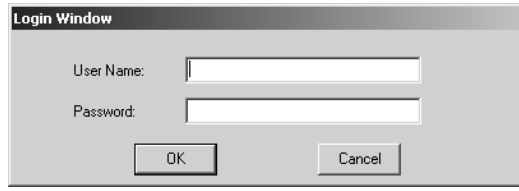


- If *Full Screen Mode* is enabled (there is a checkmark in the box), the remote display fills the entire screen of your local monitor.
- If *Full Screen Mode* is not enabled (there is no checkmark in the box), the remote display appears as a window on your desktop. If the remote screen is larger than what is able to fit in the window, move the mouse pointer to the screen border that is closest to the area you want to view and the screen will scroll.
- If *Keep Screen Size* is enabled (there is a checkmark in the box), the remote screen is not resized.
  - If the remote resolution is smaller, its display appears as a window centered on your screen.
  - If the remote resolution is larger, its display is centered on your screen. To access the areas that are off screen, move the mouse to the corner of the screen that is closest to the area you want to view and the screen will scroll.
- If *Keep Screen Size* is not enabled (there is no checkmark in the box), the remote screen is resized to fit the resolution of your local monitor.

Connecting

To connect to a CN6000 unit:

1. If it is in the *CN6000 List*, **Double Click** it; if you are using the *CN6000 IP* input box, specify the IP address and Port number, then Click **Open**. A *Login* dialog box appears:

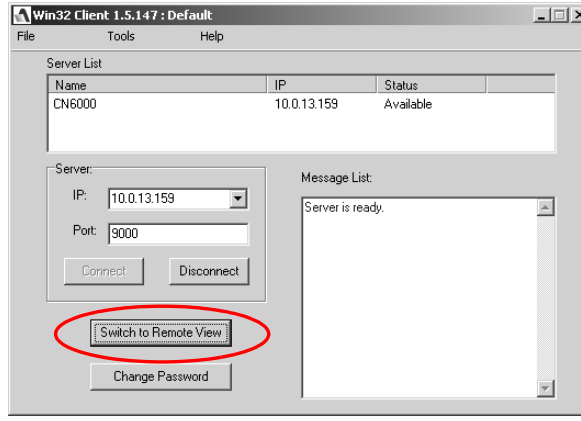


2. Key in a valid Username and Password, then click **OK**.

   The program attempts to contact your selected CN6000 unit. While it does so, you can check the *Message List* window for status messages regarding the operation's progress.

3. Once contact with the CN6000 has been established, the *Switch to Remote View* button becomes active.

   Click it to connect to the CN6000 and take over console control of the unit that is connected to it.



Operation

Once the connection to the CN6000 has been accomplished, the remote system's video output is captured and displayed on your monitor. At the same time, your local keystroke and mouse input is captured and sent to the remote system.

The look and feel of the AP Windows client operation is the same as for the browser version of the Windows client. Refer back to page 31 for details.

The Java Client

The Java Client is provided to make the CN6000 accessible to all platforms. Systems that have Java version 1.4 or higher installed can connect. If you don't already have Java, it is available for free download from Sun's Java web site (http://java.sun.com).

Starting Up

The Java-based Client software is provided on the distribution CD included with this package. Copy the Java Client *jar* file (CN6000**main.jar**) to a convenient location on your hard disk.

To bring up the Java Client Main Screen, do the following:

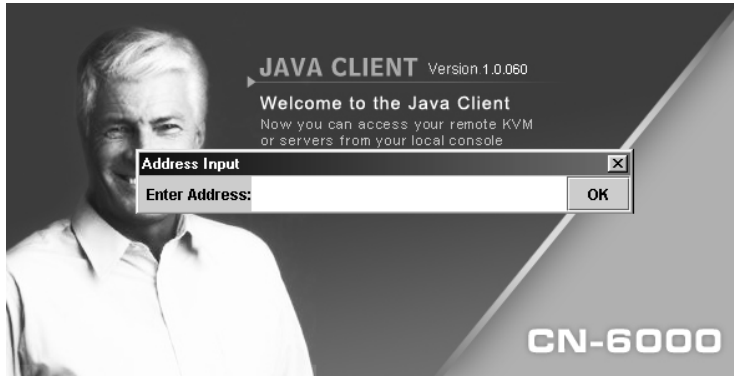
1. Copy the Java Client *jar* file (CN6000main.jar) from the CN6000 software CD to a convenient location on your hard disk.
2. Run **CN6000main.jar** either by double clicking its icon, or by keying in the full path to it on the command line.

Note: The Java Client requires Java version 1.4 or higher. It will not work with earlier versions of Java.

If this is the first time that you are running the program, a dialog box appears requesting you to input your serial number.

3. Key in the serial number - 5 characters per box - then Click **OK**. (If you don't know what the number is, contact the CN6000 administrator.)

   An *Address Input* dialog box appears:

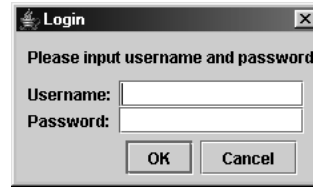


4. Key in the IP address for the unit you want to connect to - including a forward slash followed by the name of the CN6000's Java Client web page. For example:

   ```
   168.10.95.1/cn6k.html
   ```

Note: For security purposes, the name of the page that you connect to must be specified correctly as part of the IP address. The system administrator may change the name of this page from time to time to thwart unauthorized access attempts. Be sure you have the correct name for this page when you attempt to connect.

After you establish a connection, a Login dialog box appears:



5. Provide a valid Username and Password and Click **OK**.

   Once the authentication procedure completes successfully, the remote system displays your monitor:

Operation

The look and feel of the AP Java client operation is the same as for the browser version of the Java client. Refer back to page 42 for details.

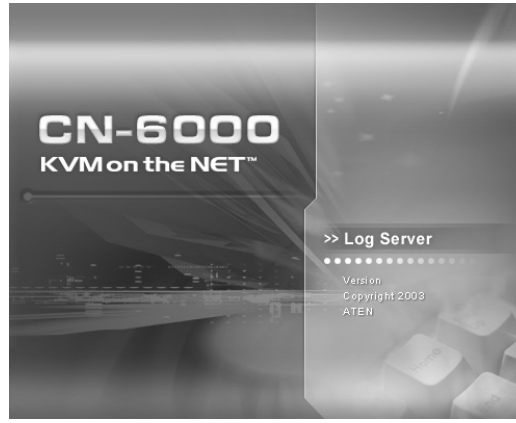
The Log Server

The Windows-based *CN6000 Log Server* is an administrative utility that records all the events that take place on selected CN6000 units.

Installation

1. Insert the CN6000 software CD into your CD-ROM drive.
2. Open the drive and folder where the Log Server Setup icon (**CN6KLogServer.exe**) is located and double click the icon.

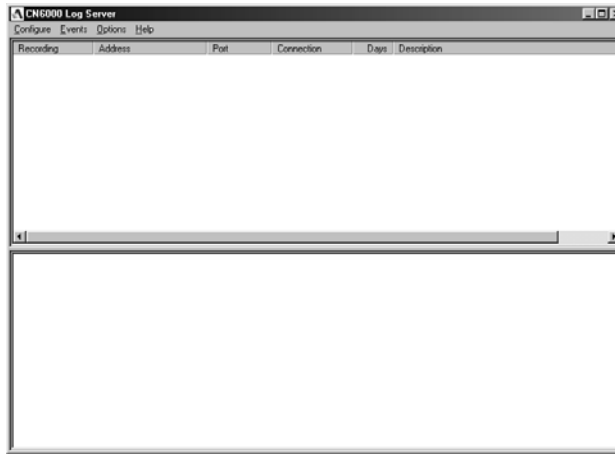
   The Log Server installation screen appears:



3. Click **Next**, and follow the on-screen instructions to complete the installation and have the program icon placed on the desktop.

Starting Up

To bring up the Log Server, run the **CN6000 Log Server** either by double clicking its icon, or by keying in the full path to CN6KLogServer.exe on the command line. A screen similar to the one below appears:



Note: The MAC address and port number of the computer that will contain the Log Server Events database must be specified on the *Network* page of the *Administrator Utility* (page 58).

The screen is divided into three components:

- A *Menu Bar* at the top
- A panel to display a list of CN6000 units below it (see page 85 for details).
- A panel to display an *Events List* at the bottom

Each of the components is explained in the sections that follow.

The Menu Bar

The Menu bar consists of four items:

- Configure
- Events
- Options
- Help

These are discussed in the sections that follow.

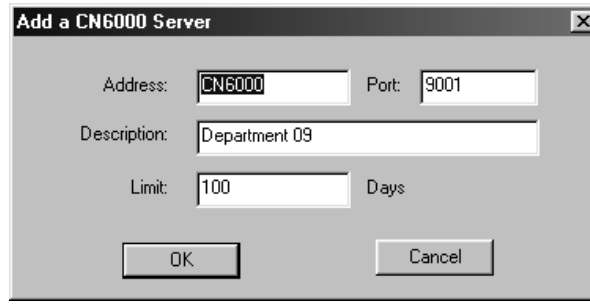
Note: If the Menu Bar appears to be disabled, click in the CN6000 List panel below it to enable the bar.

■ Configure

The Configure menu contains three items: Add; Edit; and Delete. They are used to add new CN6000 units to the CN6000 List; edit the information for units already on the list; or delete CN6000s from the list.

To edit or delete a listed CN6000, first select the one you want in the CN6000 List window, then open this menu and click **Edit** or **Delete**.

To add a CN6000 to the CN6000 List, click **Add**. When you choose *Add* or *Edit*, a dialog box, similar to the one below, appears:



A description of the fields is given in the table, below:

Field	Explanation
Address	This can either be the IP address of the CN6000 or its DNS name (if the network administrator has assigned it a DNS name).
Port	The Log Server port number assigned to the CN6000 (see *Access Ports:*, page 58).
Description	This field is provided so that you can put in a descriptive reference for the unit to help identify it.
Limit	This specifies the number of days that an event should be kept in the Log Server's database. Events that exceed the amount of time specified here, can be removed with the *Maintenance*function (see page 84 for details).

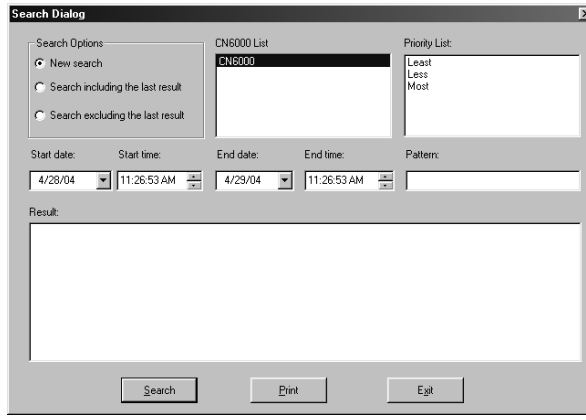
Fill in or modify the fields, then click **OK** to finish.

■ Events

The Events Menu has two items: *Search* and *Maintenance*.

Search:

Search allows you to search for events containing specific words or strings. When you access this function, a screen, similar to the one below, appears:



A description of the items is given in the table, below:

Item	Expalanation
New search	This is one of three radio buttons that define the scope of the search. If it is selected, the search is performed on all the events in the database for the selected CN6000.
Search last results	This is a secondary search performed on the events that resulted from the last search.
Search excluding last results	This is a secondary search performed on all the events in the database for the selected CN6000 *excluding*the events that resulted from the last search.
CN6000 List:	CN6000 units are listed according to their IP address. Select the unit that you want to perform the search on from this list. You can select more than one unit for the search. If no units are selected, the search is performed on all of them.
Priority	The search results are divided into three categories depending on their importance: **Most**, are events concerning System Settings and User login information, and are displayed in red. **Less**, are events concerning Network IP Settings, and are displayed in blue. **Least**, are events concerning Video Settings, and are displayed in black.
Start Date/Time	Select the date and time that you want the search to start from. The format follows the MM/DD/YYYY HH:MM:SS convention, and is numeric, as follows: `05/11/2002 13:45:08`
End Date/Time	Select the date and time that you want the search to end at.
Pattern	Key in the pattern that you are searching for here. The multiple character wildcard (%) is supported. E.g., h%ds would match *hands*and *hoods*.
Results	Lists the events that contained matches for the search.
Search	Click this button to start the search.
Print	Click this button to print the search results

Maintenance:

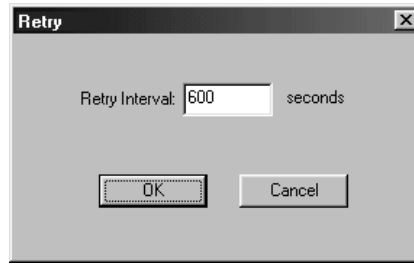
Records are not automatically erased when their time limit (see *Limit*, page 82), comes due. They still remain in the database even though they have exceeded their expiration time.

Clicking this menu item removes those records from the database.

■ Options

This menu has a single item: *Retry*.

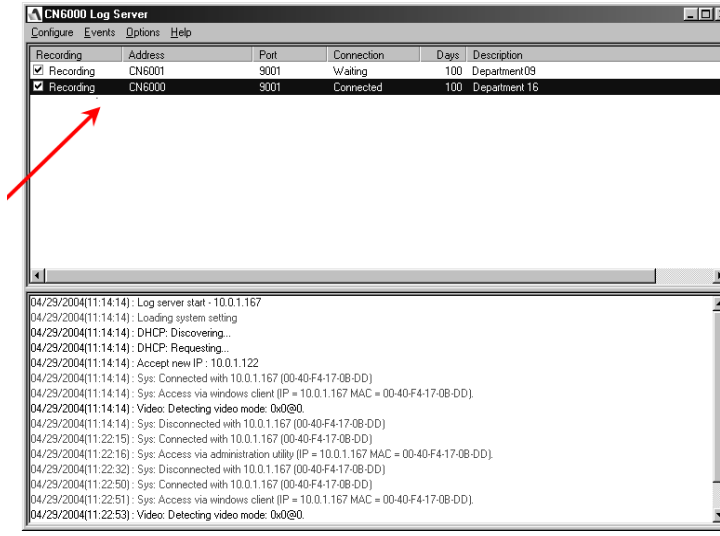
Retry allows you to set the number of seconds that the Log Server should wait before attempting to connect if its previous attempt to connect failed. When you click this item, a dialog box, similar to the one below, appears:



Key in the number of seconds, then click **OK** to finish.

The CN6000 List Panel

The CN6000 *List* panel displays a list of all the CN6000 units that have been selected for the Log Server to track (see *Configure*, page 81).


CN6000 Log Server
Configure Events Options Help
Recording Address Port Connection Days Description
Recording CN6001 9001 Waiting 100 Department 09
Recording CN6000 9001 Connected 100 Department 16
04/29/2004(11:14:14) : Log server start - 10.0.1.167
04/29/2004(11:14:14) : Loading system setting
04/29/2004(11:14:14) : DHCP: Discovering...
04/29/2004(11:14:14) : DHCP: Requesting...
04/29/2004(11:14:14) : Accept new IP : 10.0.1.122
04/29/2004(11:14:14) : Sys: Connected with 10.0.1.167 (00-40-F4-17-0B-DD)
04/29/2004(11:14:14) : Sys: Access via windows client (IP = 10.0.1.167 MAC = 00-40-F4-17-0B-DD).
04/29/2004(11:14:14) : Video: Detecting video mode: 0x0@0.
04/29/2004(11:14:14) : Sys: Disconnected with 10.0.1.167 (00-40-F4-17-0B-DD)
04/29/2004(11:22:15) : Sys: Connected with 10.0.1.167 (00-40-F4-17-0B-DD)
04/29/2004(11:22:16) : Sys: Access via administration utility (IP = 10.0.1.167 MAC = 00-40-F4-17-0B-DD).
04/29/2004(11:22:32) : Sys: Disconnected with 10.0.1.167 (00-40-F4-17-0B-DD)
04/29/2004(11:22:50) : Sys: Connected with 10.0.1.167 (00-40-F4-17-0B-DD)
04/29/2004(11:22:51) : Sys: Access via windows client (IP = 10.0.1.167 MAC = 00-40-F4-17-0B-DD).
04/29/2004(11:22:53) : Video: Detecting video mode: 0x0@0.

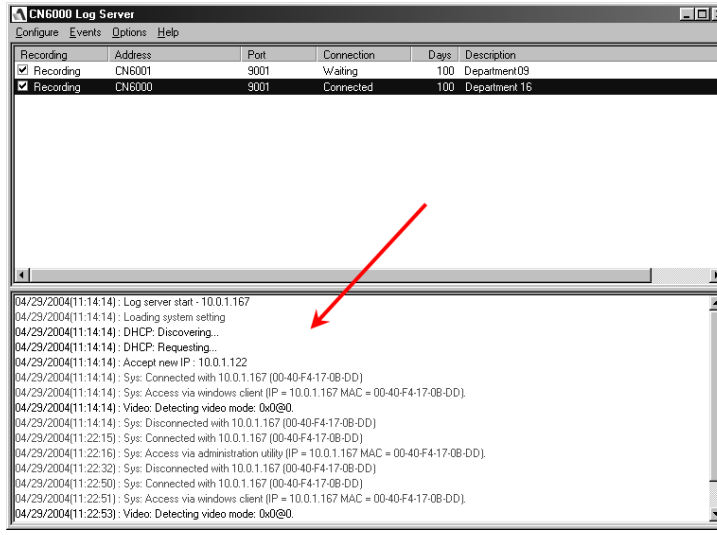
Tick information for the currently selected CN6000 displays in the *Events List* panel below it. To select a CN6000 unit in the list, simply click on it.

The CN6000 List window contains five fields:

Field	Expalanation
Recording	Determines whether the Log Server records the ticks for this CN6000, or not. If the Recording checkbox is checked, the field displays *Recording*, and the ticks are recorded.If the Recording checkbox is not checked, the field displays *Paused*, and the ticks are not recorded. **Note:**Even though a CN6000 is not the currently selected one, if its Recording checkbox is checked, the Log Server will still record its ticks.
Address	This is the IP Address or DNS name that was given to the CN6000 when it was added to the Log Server (see *Configure*, page 81).
Port	This is the Port number assigned to the CN6000 (see *Configure*, page 81).
Connection	If the Log Server is connected to the CN6000, this field displays *Connected*. If it is not connected, this field displays *Waiting*. This means that the Log Server's MAC address has not been set properly. It needs to be set on the *Network* page of the *Administrator Utility* (see page 58).
Days	This field displays the number of days that the CN6000's events are to be kept in the Log Server's database before expiration (see *Configure*, page 81).
Description	This field displays the descriptive information given for the CN6000 when it was added to the Log Server (see *Configure*, page 81).

The Event List Window

This window displays tick information for the currently selected CN6000.


CN6000 Log Server
Configure Events Options Help
Recording Address Port Connection Days Description
Recording CN6001 9001 Waiting 100 Department09
Recording CN6000 9001 Connected 100 Department 16
04/29/2004(11:14:14) : Log server start - 10.0.1.167
04/29/2004(11:14:14) : Loading system setting
04/29/2004(11:14:14) : DHCP: Discovering...
04/29/2004(11:14:14) : DHCP: Requesting...
04/29/2004(11:14:14) : Accept new IP : 10.0.1.122
04/29/2004(11:14:14) : Sys: Connected with 10.0.1.167 (00-40-F4-17-0B-DD)
04/29/2004(11:14:14) : Sys: Access via windows client (IP = 10.0.1.167 MAC = 00-40-F4-17-0B-DD).
04/29/2004(11:14:14) : Video: Detecting video mode: 0x0@0.
04/29/2004(11:14:14) : Sys: Disconnected with 10.0.1.167 (00-40-F4-17-0B-DD)
04/29/2004(11:22:15) : Sys: Connected with 10.0.1.167 (00-40-F4-17-0B-DD)
04/29/2004(11:22:16) : Sys: Access via administration utility (IP = 10.0.1.167 MAC = 00-40-F4-17-0B-DD).
04/29/2004(11:22:32) : Sys: Disconnected with 10.0.1.167 (00-40-F4-17-0B-DD)
04/29/2004(11:22:50) : Sys: Connected with 10.0.1.167 (00-40-F4-17-0B-DD)
04/29/2004(11:22:51) : Sys: Access via windows client (IP = 10.0.1.167 MAC = 00-40-F4-17-0B-DD).
04/29/2004(11:22:53) : Video: Detecting video mode: 0x0@0.

Note that even though any other CN6000s aren't currently selected, if their *Recording* checkbox is checked, the Log Server records their tick information and keeps it in its database. You can see the server's tick information by selecting it.

Appendix

Specifications

Function			Specification
Connectors	Console Ports	Keyboard	1 x 6 pin mini-DIN Female (Purple)
		Video	1 x HDB-15 Female (Blue)
		Mouse	1 x 6 pin mini-DIN Female (Green)
	KVM Link		1 x SPHD-15 F
	LAN		1 x RJ-45 Receptacle
	PON[1]		1 x RS-232
	Power		1 x DC Jack (5V; 2.6A)
LEDs	Power		1 (Orange)
	Link		1 (Green)
	10/100 Mbps		1 (Green/Orange)
Video			Up to 1600 x 1200 @ 60 Hz
Power Consumption			DC5V; 7W
Protocols			10BaseT Ethernet; 100BaseT Fast Ethernet; TCP/IP; HTTP
Environment	Operating Temp.		0—50° C
	Storage Temp.		-20—60° C
	Humidity		0—80% RH
Physical Properties	Housing		Metal
	Weight		0.51kg
	Dimensions (L x W x H)		20 x 8 x 2.5 cm

1 Power Over the Net

IP Address Determination

If you are an administrator logging in for the first time, you need to access the CN6000 in order to give it an IP address that users can connect to. There are three methods to choose from. In each case, your computer must be on the same network segment as the CN6000. If the CN6000's address was set by DHCP, Method 3 will show you what the DHCP assigned address is.

After you have connected and logged in you can give the CN6000 its fixed network address in the *Network Settings* dialog box (see page 17). If you want to have the CN6000's address set by DHCP and the address changes, use Method 3 to determine the new address.

Method 1: (For a fixed IP address)

When the CN6000 starts, if it doesn't find a DHCP environment after 30 seconds, it automatically sets its IP address to 192.168.0.60.

1. Set your computer's IP address to 192.168.0.*XXX*

   Where *XXX* represents any number or numbers except 60.

2. Specify the switch's default IP address (192.168.0.60) in the URL entry box of your browser.

3. After you connect and log in, assign a fixed IP address for the CN6000 that is suitable for the network segment that it resides on.

4. After you log out, be sure to reset your computer's IP address to its original value.

Method 2: (For a fixed IP address)

A fixed IP address can also be assigned with the ARP command as follows:

1. If the CN6000 is powered on, Power it off by unplugging its power adapter cable.
2. Run the ARP command with the following arguments:

   ```
   arp -s <desired ip address> <CN6000's MAC address>
   ```

   Where the IP address that you assign is one suitable for the network segment that the CN6000 resides on.

   Note: The CN6000's MAC address can be found on its bottom panel.

3. Power on the CN6000
4. From your browser, log into the CN6000 using the IP address you just assigned.

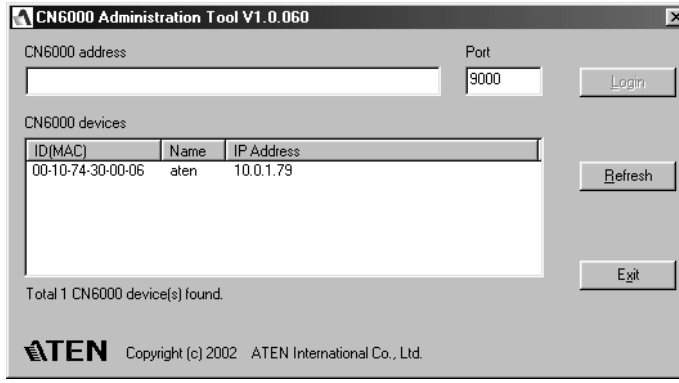
   Note: You must do this within 30 seconds of powering the CN6000 on.

Method 3: (For a DHCP address)

For computers running Windows, the CN6000's DHCP generated IP address can be determined with the *AdminTool* utility (found on the distribution CD):

1. Double click the AdminTool utility icon on the CD to install the utility on your computer. When the installation completes, there is a *CN6000 AdminTool* icon on your desktop.
2. Double click the CN6000 AdminTool icon.

   The utility searches the network segment for CN6000 devices, and displays what it finds in a dialog box similar to the one below:



   The DHCP assigned IP address appears in the right hand column of the *CN6000 Devices* panel:

Note: 1. .If there is more than one device in the list, use the MAC address to pick the one you want. The CN6000's MAC address is located on its bottom panel.

2. If the list is empty, or your device doesn't appear, click **Refresh** to refresh the Device List.

3. Click **Exit** to close the utility.

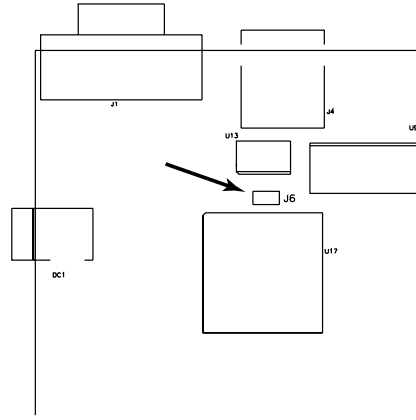
Administrator Login Failure

If you are unable to perform an Administrator login (because the Username and Password information has become corrupted, or you have forgotten it, for example), there is a procedure you can use to clear the login information.

Note: Performing this procedure also returns all settings to their defaults.

To clear the login information (and return all settings to their defaults), do the following:

1. Power off the CN6000 and remove its housing.
2. Short the jumper on the mainboard labeled J6.



3. Power on the switch.
4. When the front panel LEDs flash, power off the switch.
5. Remove the jumper cap from J6.
6. Close the housing and start the CN6000 back up.

   After you start back up, you can use the default Username and Password (see page 12) to log in.

Troubleshooting

General Operation

Problem	Resolution
Erratic Operation	If the CN6000 is connected to a KVM switch, make sure to power on the switch before powering on the CN6000.
	Press and hold the Reset button (see page 5), for longer than three seconds.
Mouse Pointer Confusion	If you find the display of two mouse pointers (local and remote) to be confusing or annoying, you can use the *Toggle Mouse Display* function to shrink the non-functioning pointer. See p. 35 for details.

The Windows Client

Problem	Resolution
Windows Client won't connect to the CN6000.	DirectX 7.0 or higher must be installed on your computer.
Remote mouse pointer is out of step.	1. Use the *AutoSync* feature (see *Video Adjustment*, page 36), to synch the local and remote monitors. 2. If that doesn't resolve the problem, use the *Adjust Mouse* feature (see *Mouse Synchronization*, page 32) to bring them back in step. 3. If the two methods shown above fail to resolve the problem, use the *Toggle Mouse Display* function (see page 35).
Part of remote window is off my monitor.	If *Keep Screen Size* (see page 30) is not enabled, use the *AutoSync* feature (see *Video Adjustment*, page 36), to sync the local and remote monitors. If it is enabled, see the discussion under *Keep Screen Size*, page 30.
The remote screen display is rotated 90^{o}	Enable *Keep Screen Size*. See the discussion under *Keep Screen Size*, page 30.
I can't run Net Meeting when the Windows Client is running.	Enable *Keep Screen Size*. See the discussion under *Keep Screen Size*, page 30.
When I log in, the browser generates a *CA Root certificate is not trusted*, or a *Certificate Error* response.	The certificate's name is not found on Microsoft's list of Trusted Authorities. The certificate can be trusted. See *Trusted Certificates*, page 97, for details.

Sun Systems

Problem	Resolution

Video display problems with HDB15 interface systems (e.g., Sun Blade 1000 servers).[1]	The display resolution should be set to 1024 x 768:
	Under Text Mode:
	1. Go to **OK mode** and issue the following commands:
	`setenv output-device screen:r1024x768x60`
	`reset-all`
	Under XWindow:
	1. Open a console and issue the following command:
	`m64config -res 1024x768x60`
	2. Log out
	3. Log in

Video display problems with 13W3 interface systems (e.g., Sun Ultra servers).*	The display resolution should be set to 1024 x 768:
	Under Text Mode:
	1. Go to **OK mode** and issue the following commands:
	`setenv output-device screen:r1024x768x60`
	`reset-all`
	Under XWindow:
	1. Open a console and issue the following command:
	`m64config -res 1024x768x60`
	2. Log out
	3. Log in

***** These solutions work for most common Sun VGA cards. If using them fails to resolve the problem, consult the Sun VGA card's manual.

The Java Client

For mouse synchronization problems, see *Mouse:*, page 44. For connection and operation problems, see the table below:

Symptom	Action
Java Client won't connect to the CN6000	1. Java 2 JRE 1.4 or higher must be installed on your computer. 2. Make sure to include the correct default java program name when you specify the CN6000's IP address. 3. Close the Java Client, reopen it, and try again.
Java Client performance deteriorates.	Exit the program and start again.
National language characters don't appear.	When entering national language characters, if your local keyboard is set to a non-English national language layout, you must set the remote computer's keyboard layout to English.
When I log in, the browser generates a *CA Root certificate is not trusted*, or a *Certificate Error* response.	The certificate's name is not found on Microsoft's list of Trusted Authorities. The certificate can be trusted. See *Trusted Certificates*, page 97, for details.

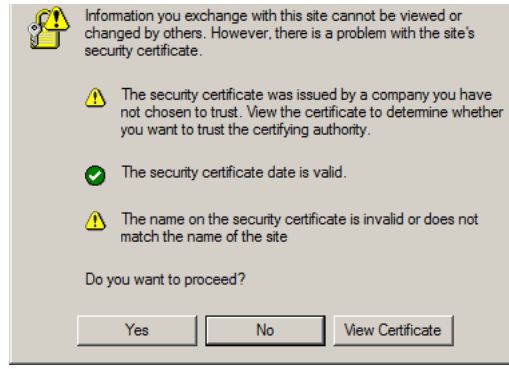
The Log Server

Problem	Resolution
The Log Server program does not run.	The Log Server requires the Microsoft Jet OLEDB 4.0 driver in order to access the database. This driver is automatically installed with Windows ME, 2000 and XP. For Windows 98 or NT, you will have to go to the Microsoft download site: http://www.microsoft.com/data/download.htm to retrieve the driver file: MDAC 2.7 RTM Refresh (2.70.9001.0) Since this driver is used in Windows Office Suite, an alternate method of obtaining it is to install Windows Office Suite. Once the driver file or Suite has been installed, the Log Server will run.

Trusted Certificates

Overview

When you try to log in to the device from your browser, a Security Alert message appears to inform you that the device's certificate is not trusted, and asks if you want to proceed.


Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

The certificate can be trusted, but the alert is triggered because the certificate's name is not found on Microsoft's list of Trusted Authorities. You have two options: 1) you can ignore the warning and click **Yes** to go on; or 2) you can install the certificate and have it be recognized as trusted.

- If you are working on a computer at another location, accept the certificate for just this session by clicking **Yes.**
- If you are working at your own computer, install the certificate on your computer (see below for details). After the certificate is installed, it will be recognized as trusted.

Limited Warranty

IN NO EVENT SHALL THE DIRECT VENDOR'S LIABILITY EXCEED THE PRICE PAID FOR THE PRODUCT FROM THE DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, DISK OR ITS DOCUMENTATION.

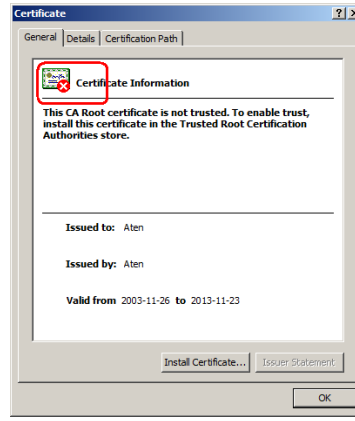
The direct vendor makes no warranty or representation, expressed, implied, or statutory with respect to the contents or use of this documentation, and specially disclaims its quality, performance, merchantability, or fitness for any particular purpose.

The direct vendor also reserves the right to revise or update the device or documentation without obligation to notify any individual or entity of such revisions, or update. For further inquires please contact your direct vendor.

Installing the Certificate

To install the certificate, do the following:

1. In the *Security Alert* dialog box, click **View Certificate.** The *Certificate Information* dialog box appears:



Note: There is a red and white **X** logo over the certificate to indicate that it is not trusted.

2. Click **Install Certificate.**
3. Follow the Installation Wizard to complete the installation. Unless you have a specific reason to choose otherwise, accept the default options.
4. When the Wizard presents a caution screen:

Security Warning
You are about to install a certificate from a certification authority (CA) claiming to represent:
Aten
Windows cannot validate that the certificate is actually from "Aten". You should confirm its origin by contacting "Aten". The following number will assist you in this process:
Thumbprint (sha1): F3B66988 A134DD25 1E6F09BC 895F6DCD B30FB7AF
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.
Do you want to install this certificate?
Yes
No

Click **Yes**.

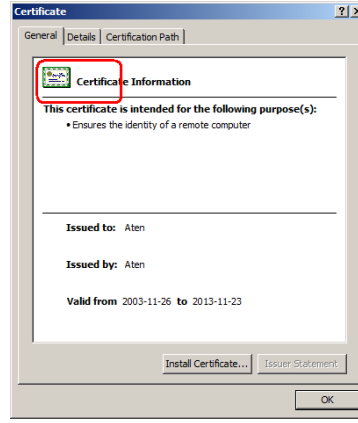
5. Next, click **Finish** to complete the installation; then click **OK** to close the dialog box.

Certificate Trusted

The certificate is now trusted:

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate is from a trusted certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

When you click *View Certificate*, you can see that the red and white **X** logo is no longer present – further indication that the certificate is trusted:



This Page Intentionally Left Blank

Index

A

Administration, 15
- Customization, 26
- Filtering, 20
- Firmware upgrading, 27
- General, 16
- Network, 17
- RADIUS settings, 22
- Security, 19
- User Manager, 24

Administrator Login Failure, 93
Administrator Utility, 51
- Customization, 65
- Installation, 51
- Logging in, 53
- Settings Notebook, 55
- Starting up, 52
- User Management, 63

AP Operation, 51
Autosync, 43

B

Browser screen elements, 14

C

Cable sets, 4
CN-6000
- Front view, 5
- Rear view, 6

Components
- Rear View, 6

Config, 73
Configure
- Log Server, 81

Windows Client, 74
Corrupt Password, 93
Customization, 26

F

Features, 3
Filtering, 19, 20, 60, 61
Firmware
- Upgrading, 65, 66

Firmware upgrading, 27
Forgotten Password, 93

G

Getting Started, 11

H

Hardware Setup
- Front View, 5
- Installation, 9

Hotkey Setup Screen, 34
Hotkeys
- Windows Client, 34, 72

I

Installation, 9
Invalid login, 12, 54
IP address determination, 90
IP filtering, 20

J

Java Client, 41, 76
- Keypad, 44
- Login, 78
- Operation, 42, 78
- Starting Up, 76
- Toolbar, 43
- Troubleshooting, 96

L

Log File
Main Screen, 49
Log file, 49
Log Server, 2, 18, 59
CN-6000 List Panel, 85
Configure, 81
Event List Window, 87
Events, 82
Installation, 79
Main Screen, 80
Maintenance, 84
Menu Bar, 81
Options, 84
Search, 82
Starting Up, 80
Troubleshooting, 96
Logging In, 11
Login
Failure, 26
Invalid login, 12, 54

M

MAC Address, 16
MAC filtering, 21
Message Board
Java Client, 45
Windows Client, 38
Mouse Synchronization, 32, 44

N

Network, 17
Network environment, 58

O

Overview, 1

R

Rack Mounting, 7
Safety information, vi
RADIUS settings, 22
Reset on exit, 26

S

Safety Instructions
General, iv
Rack Mounting, vi
Screen Elements, 14
Security, 19
Serial number, 52
Java Client, 76
Settings Notebook, 55
General, 57
Network, 58
Security, 60
Uploading Changes, 56
Substitute keys, 32
Substitute Keystrokes, 32
System Requirements, 4

T

Time out control, 26
Troubleshooting
Java Client, 96
Log Server, 96
Windows Client, 94
Trusted Certificates, 97

U

Upgrading firmware, 65
Upgrading the Firmware, 66
User Management, 63
User Manager, 24
User Station filtering
IP, 20
MAC, 21

V

Video Adjustment
Java Client, 43
Windows Client, 36

W

Windows Client, 2, 29, 68
Config, 73
Connection screen, 69
Control Panel], 31
File menu, 71
Hotkeys, 34, 72
Installation, 68
Logging in, 74
Main Screen, 69
Operation, 31, 75
Starting up, 29, 69
Substitute keys, 32
Tools menu, 72
Troubleshooting, 94

Contents

FCC Information ii
User Notice iii
Safety Instructions iv
General iv
Rack Mounting vi
Package Contents vii
Basic Package vii
Optional Equipment vii
About this Manual xi
Conventions xii
ATEN Information xii
Online Registration xii
Online Support xii

1. Introduction

Overview 1
Features 3
System Requirements 4
Components 5
Front View 5
Rear View 6

2. Hardware Setup

Rack Mounting 7
Installation 9

3. Getting Started

Logging In 11
Screen Elements 14

4. Administration

Introduction 15
General 16
Network 17
Access Port 17
IP Address 18
DNS Server 18
Log Server 18
Security 19
Filtering 20
Radius 22
User Manager 24
Customization 26
Firmware 27

5. The Windows Client

Starting Up 29
Operation 31
OSD Control Panel 31
Keystrokes 32
Mouse Synchronization 32
Hotkeys 34
Configuring the Hotkeys 35
Video Adjustment 36
The Message Board 38
The Button Bar 39
Message Display Panel 39
Compose Panel 39
User List Panel 40

6. The Java Client

Introduction 41
Operation 42
The Toolbar 43

7. The Log File

The Log File Screen 49

8. AP Operation

The Administrator Utility 51
Installation 51
Starting Up 52
Logging In 53
The Settings Notebook 55
Uploading Changes 56
General: 57
Network: 58
Security 60
Filtering 61
User Management 63
Customization 65
Upgrading the Firmware 66
The Windows Client 68
Installation 68
Starting Up 69
The Connection Screen 69
The File Menu 71
The Tools Menu 72
Keyboard 72
Config 73

Connecting 74
Operation 75
The Java Client 76
Starting Up 76
Operation 78
The Log Server 79
Installation 79
Starting Up 80
The Menu Bar 81
Configure 81
Events 82
Options 84
The CN6000 List Panel 85
The Event List Window 87

9. Appendix

Specifications 89
IP Address Determination 90
Administrator Login Failure 93
Troubleshooting 94
General Operation 94
The Windows Client 94
Sun Systems 95
The Java Client 96
The Log Server 96
Trusted Certificates 97
Overview 97
Installing the Certificate 98
Certificate Trusted 99